T2

Machine Learning

Salvador Ruiz Correa

January 19, 2026

This brief review synthesizes key mathematical structures that form the conceptual backbone of machine learning. We begin with fundamental algebraic structures—groups, rings, and fields—culminating in the definition of a vector space, where data are typically represented. Essential vector space concepts such as linear independence, span, and basis are introduced, highlighting their role in feature representation.

The discussion then progresses to structures that equip vector spaces with analytical tools: metric spaces for measuring similarity, normed spaces for vector magnitude, and inner product spaces for angles and orthogonality. This sequence leads to Hilbert spaces—complete inner product spaces central to functional analysis and machine learning theory. Within Hilbert spaces, we outline the orthogonal projection theorem, which underpins optimization and approximation methods, and the Riesz representation theorem, linking linear functionals to inner products, a foundation for kernel methods.

Finally, we introduce Mercer's theorem, which connects positive-definite kernels to inner products in Hilbert spaces, thereby enabling the kernel trick—a pivotal technique for transforming nonlinear problems into linear ones in higher-dimensional spaces. This concise journey illustrates how abstract mathematical frameworks provide the rigorous foundations for many algorithms and theoretical guarantees in machine learning.

Agenda:

1. Algebraic Structures.
2. Spaces (metric, normed, inner-product, Hilbert.
3. Mercer Theorem.

Introduction

Machine Learning (ML) models data mathematically. To understand the core algorithms (linear regression, SVMs, neural network layers), we must first understand the **structures** in which data "lives." We begin with the most abstract building blocks and build up to the essential concept of a **vector space**.

Basic Algebraic Structures

These structures define sets equipped with operations obeying specific axioms.

Groups

A group formalizes symmetry and reversible transformations.

Definition 1: Group

Definition 1 (Group) *A **group** $(G, *)$ is a set G with a binary operation $* : G \times G \to G$ such that:*

1. ***Closure:*** $\forall a, b \in G,\ a * b \in G$.
2. ***Associativity:*** $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$.
3. ***Identity:*** $\exists e \in G$ *such that* $\forall a \in G,\ a * e = e * a = a$.
4. ***Inverse:*** $\forall a \in G,\ \exists b \in G$ *such that* $a * b = b * a = e$. *(We write* $b = a^{-1}$*).*

If $\forall a, b, a * b = b * a$*, the group is **abelian** (commutative).*

Example 1 $(\mathbb{Z}, +)$ *is an abelian group (identity 0, inverse* $-n$*).* $(\mathbb{R} \setminus \{0\}, \times)$ *is an abelian group (identity 1, inverse* $1/x$*).*

ML Context: The set of all permutations of data features forms a (non-abelian) group.

Rings

Rings have two operations, often thought of as addition and multiplication.

Definition 2: Ring

Definition 2 (Ring) *A **ring** $(R, +, \cdot)$ is a set R with two operations such that:*

1. $(R, +)$ *is an **abelian group** (identity denoted 0).*
2. ***Multiplication Associativity:*** $\forall a, b, c \in R,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. ***Distributivity:*** $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c$.

If multiplication is commutative $(a \cdot b = b \cdot a)$*, it's a **commutative ring**. If there is a multiplicative identity (denoted 1), it's a **ring with unity**.*

Example 2 $\mathbb{Z}$ *(integers),* $\mathbb{R}^{n \times n}$ *(square matrices) are rings. Matrices show a non-commutative ring.*

ML Context: The arithmetic of weights and inputs in a model often occurs in a ring.

Fields

Fields are rings where division (except by zero) is possible.

Definition 3: Fields

Definition 3 (Field) *A **field** $\mathbb{F}$ is a commutative ring with unity where every non-zero element has a multiplicative inverse. Formally, $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group.*

Example 3 *$\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) are fields. $\mathbb{Z}$ is **not** a field (no inverse for 2 in $\mathbb{Z}$).*

ML Context: Almost all numerical ML uses real numbers $\mathbb{R}$ or sometimes complex numbers $\mathbb{C}$ as the underlying scalar field.

Vector Spaces: Where Data Lives

A vector space combines a field of scalars with an abelian group of vectors.

Definition 4: Vector Space

Definition 4 (Vector Space) *Let $\mathbb{F}$ be a field. A **vector space** V over $\mathbb{F}$ is a set V equipped with:*

- ***Vector Addition:*** *$+ : V \times V \to V$, making $(V, +)$ an **abelian group**.*
- ***Scalar Multiplication:*** *$\cdot : \mathbb{F} \times V \to V$.*

These operations must satisfy $\forall \alpha, \beta \in \mathbb{F}$, $\mathbf{u}, \mathbf{v} \in V$:

1. $\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \alpha\mathbf{v}$
2. $(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$
3. $(\alpha\beta)\mathbf{u} = \alpha(\beta\mathbf{u})$
4. $1 \cdot \mathbf{u} = \mathbf{u}$ *(where 1 is the multiplicative identity in $\mathbb{F}$)*

Example 4 *$\mathbb{R}^n$ over $\mathbb{R}$ is the canonical example. The set of all $m \times n$ matrices over $\mathbb{R}$ is a vector space. Functions $f : \mathbb{R} \to \mathbb{R}$ also form a vector space.*

ML Context: A single data point with n features is a vector in $\mathbb{R}^n$. A dataset of m points is a set (or matrix) of vectors.

Essential Vector Space Concepts

Linear Combination, Span, and Subspaces

Definition 5 (Linear Combination) *Given vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in V$ and scalars $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$, the vector $\alpha_1\mathbf{v}_1 + \ldots + \alpha_k\mathbf{v}_k$ is a **linear combination**.*

Definition 6 (Span) *The **span** of a set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is the set of all* *linear combinations of those vectors:*

$$span(S) = \left\{ \sum_{i=1}^{k} \alpha_i \mathbf{v}_i : \alpha_i \in \mathbb{F} \right\}.$$

This is always a ***subspace*** *(a vector space contained within V).*

ML Context: The span represents all possible points that can be constructed (e.g., modeled) using a given set of feature vectors. A model's hypothesis space is often a subspace.

Linear Independence and Basis

Definition 7 (Linear Independence) *A set $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is* ***linearly independent*** *if the equation*

$$\alpha_1 \mathbf{v}_1 + \ldots + \alpha_k \mathbf{v}_k = \mathbf{0}$$

has ***only*** *the trivial solution $\alpha_1 = \ldots = \alpha_k = 0$. Otherwise, the set is* ***linearly dependent****.*

Interpretation: Independence means no vector in S is redundant; it cannot be written as a combination of the others.

Definition 8 (Basis and Dimension) *A* ***basis*** *$\mathcal{B}$ for a vector space V is a set of vectors that is:*

1. ***Linearly Independent***
2. ***Spans*** *V (i.e., $span(\mathcal{B}) = V$)*

The ***dimension*** *$dim(V)$ is the number of vectors in any basis for V. Every vector $\mathbf{v} \in V$ can be expressed* ***uniquely*** *as a linear combination of basis vectors.*

Example 5 *The* ***standard basis*** *for $\mathbb{R}^3$: $\mathcal{B} = \{(1,0,0), (0,1,0), (0,0,1)\}$. Any vector $(x, y, z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$.*

Role in Feature Representation

This is the core connection to ML:

- **Feature Vector:** A data point $\mathbf{x} = [x_1, \ldots, x_n]^T \in \mathbb{R}^n$ is a vector.
- **Feature Space:** The vector space $\mathbb{R}^n$ is the **feature space**.
- **Basis as Feature Directions:** Each basis vector $\mathbf{e}_i$ can represent a fundamental, independent **direction** or **concept** in the feature space (e.g., "pixel intensity at location i," "word count for word i").
- **Coefficients as Representations:** The coordinates $(x_1, \ldots, x_n)$ of $\mathbf{x}$ relative to the standard basis *are* the feature values. Changing the basis is like changing the **perspective** or **coordinate system** for viewing the data.

- **Dimensionality Reduction:** If your data points are linearly dependent, the true "intrinsic" dimension is less than n. Finding a smaller basis that *approximately* spans the data (e.g., via PCA) is the goal of dimensionality reduction.

Summary

We built a hierarchy: **Group** $\to$ **Ring** $\to$ **Field** $\to$ **Vector Space**.
- A vector space over a field is the primary stage for numerical data.
- Concepts of **span, linear independence, and basis** allow us to discuss representation, dimensionality, and transformations of data.

Metric Spaces

Definition 5: Metric Space

Definition 9 (Metric Space) *A **metric space** is an ordered pair (X, d) consisting of:*
- *A set X (whose elements are called "points")*
- *A function $d : X \times X \to \mathbb{R}$ (called a **metric** or **distance function**)*

satisfying the following axioms for all $x, y, z \in X$:
1. *Non-negativity: $d(x, y) \geq 0$*
2. *Identity of indiscernibles: $d(x, y) = 0 \iff x = y$*
3. *Symmetry: $d(x, y) = d(y, x)$*
4. *Triangle inequality: $d(x, z) \leq d(x, y) + d(y, z)$*

Types of Distances (Metrics)

Standard Metrics on $\mathbb{R}^n$

Definition 10 (ℓ^p Metrics) *For $p \geq 1$, the ℓ^p metric on $\mathbb{R}^n$ is:*

$$d_p(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{1/p}$$

where $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$.

Example 6 (Important Special Cases) *1. **Euclidean distance** (ℓ^2 metric):*

$$d_2(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

2. ***Manhattan distance*** *(ℓ^1 metric):*

$$d_1(x, y) = \sum_{i=1}^{n} |x_i - y_i|$$

3. ***Chebyshev distance*** *(ℓ^∞ metric):*

$$d_\infty(x, y) = \max_{1 \le i \le n} |x_i - y_i|$$

Discrete Metric

Definition 11 (Discrete Metric) *For any set X, the **discrete metric** is:*

$$d(x, y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases}$$

Example 7 *On $X = \{a, b, c\}$:*

$$d(a, b) = 1, \quad d(b, c) = 1, \quad d(a, c) = 1, \quad d(a, a) = 0$$

All distinct points are exactly "1 unit" apart.

Metrics on Function Spaces

Definition 12 (Uniform Metric) *On $C[a, b]$ (continuous functions on $[a, b]$):*

$$d_\infty(f, g) = \sup_{x \in [a,b]} |f(x) - g(x)|$$

*Also called the **supremum metric** or **Chebyshev metric**.*

Definition 13 (L^p Metrics) *On appropriate function spaces:*

$$d_p(f, g) = \left(\int_a^b |f(x) - g(x)|^p dx \right)^{1/p}$$

Special cases:

- $p = 1$: $d_1(f, g) = \int_a^b |f(x) - g(x)| dx$ *(total area between curves)*
- $p = 2$: $d_2(f, g) = \sqrt{\int_a^b |f(x) - g(x)|^2 dx}$ *(root mean square distance)*

Metrics on Sequence Spaces

Definition 14 (ℓ^p Sequence Spaces) *For sequences $(a_n), (b_n)$:*

$$d_p((a_n), (b_n)) = \left(\sum_{n=1}^{\infty} |a_n - b_n|^p \right)^{1/p}$$

provided the sum converges.

Specialized Metrics

Definition 15 (Hamming Distance) *For strings of equal length $x, y \in \{0,1\}^n$ (or any alphabet):*

$$d_H(x,y) = \text{number of positions where } x_i \neq y_i$$

Definition 16 (Cosine Distance) *For vectors $x, y \in \mathbb{R}^n$:*

$$d_{cos}(x,y) = 1 - \frac{\langle x,y \rangle}{\|x\| \, \|y\|}$$

where $\langle x,y \rangle$ is the dot product.

Definition 17 (Mahalanobis Distance) *For vectors $x, y \in \mathbb{R}^n$ with covariance matrix Σ:*

$$d_M(x,y) = \sqrt{(x-y)^T \Sigma^{-1} (x-y)}$$

Appendix 1. Modules

A **module** is a fundamental algebraic structure that generalizes the concept of a vector space. While vector spaces are defined over fields, modules are defined over rings. This generalization makes modules more flexible but also more complex.

The Need for Modules

- **Vector spaces**: Require a **field** as the scalar set
- **Modules**: Allow a **ring** as the scalar set
- **Key difference**: In a ring, not all elements have multiplicative inverses, making modules more general but with more subtle structure

Formal Definition

Definition 18 (Module over a Ring) *Let R be a **ring** (with unity 1_R). A **left R-module** is an abelian group $(M, +)$ together with a scalar multiplication operation:*

$$\cdot : R \times M \to M$$

denoted $(r, m) \mapsto r \cdot m$ or simply rm, satisfying for all $r, s \in R$ and $m, n \in M$:

(i) ***Distributivity over module addition**:*

$$r(m+n) = rm + rn$$

(ii) ***Distributivity over ring addition**:*

$$(r+s)m = rm + sm$$

(iii) ***Compatibility with ring multiplication:***

$$(rs)m = r(sm)$$

(iv) ***Identity action:***

$$1_R \cdot m = m$$

We denote this structure as ${}_RM$ (left module) or simply M when the ring is clear.

Appendix 2. Rotations in 2-D and 3-D

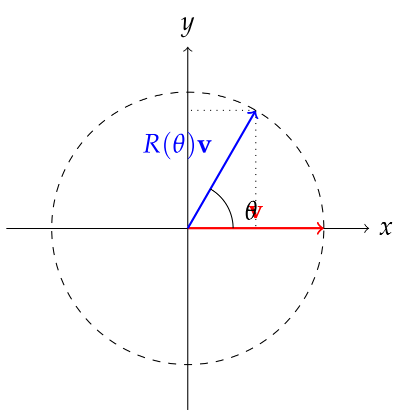
Rotations in Euclidean space provide excellent examples of mathematical groups. While 2D rotations form a simple abelian group, 3D rotations exhibit richer, non-abelian structure. Both are crucial in physics, computer graphics, and machine learning.

Rotations in Two Dimensions

A rotation in the plane by angle θ about the origin can be represented in multiple equivalent ways:

1. **As an angle**: $\theta \in [0, 2\pi)$ or $\mathbb{R} \mod 2\pi$
2. **As a complex number**: $e^{i\theta} = \cos\theta + i\sin\theta$ on the unit circle
3. **As a 2x2 matrix**:

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$



2D Rotations Form a Group

Let $G = \{R(\theta) : \theta \in \mathbb{R} \mod 2\pi\}$ with matrix multiplication as the group operation.

Proof 1 (Verification of Group Axioms) *1.* ***Closure:***

$$R(\theta_1)R(\theta_2) = \begin{pmatrix} \cos\theta_1 & -\sin\theta_1 \\ \sin\theta_1 & \cos\theta_1 \end{pmatrix} \begin{pmatrix} \cos\theta_2 & -\sin\theta_2 \\ \sin\theta_2 & \cos\theta_2 \end{pmatrix} = R(\theta_1 + \theta_2) \in G$$

2. ***Associativity***: *Matrix multiplication is associative.*
3. ***Identity***:

$$R(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

4. ***Inverse***:

$$R(\theta)^{-1} = R(-\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

since $R(\theta)R(-\theta) = R(0) = I_2$.

Properties of the 2D Rotation Group

- **Abelian (commutative)**:

$$R(\theta_1)R(\theta_2) = R(\theta_1 + \theta_2) = R(\theta_2 + \theta_1) = R(\theta_2)R(\theta_1)$$

- **Isomorphic to the circle group**:

$$\mathrm{SO}(2) \cong U(1) \cong S^1$$

where SO(2) = Special Orthogonal group in 2D, $U(1)$ = unitary complex numbers, S^1 = unit circle.
- **One-dimensional**: Parameterized by a single parameter θ.

Rotations in Three Dimensions

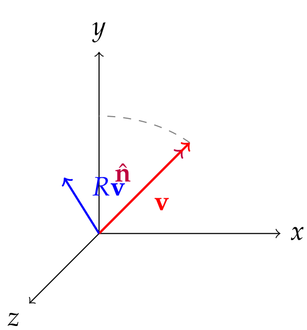
Representation of 3D Rotations

3D rotations are more complex due to non-commutativity. They can be represented as:

1. **Axis-angle representation**: $(\hat{\mathbf{n}}, \theta)$ where $\hat{\mathbf{n}}$ is a unit vector (axis) and θ is the angle.
2. **3×3 rotation matrices**: Elements of SO(3), satisfying:

$$R^T R = I_3 \quad \text{and} \quad \det(R) = 1$$

3. **Quaternions**: $q = \cos(\theta/2) + \sin(\theta/2)(n_x i + n_y j + n_z k)$



SO(3): The 3D Rotation Group

Let SO(3) = $\{R \in \mathbb{R}^{3\times 3} : R^T R = I_3, \det(R) = 1\}$ with matrix multiplication.

Proof 2 (Verification of Group Axioms) *1. **Closure**: If $R_1, R_2 \in SO(3)$, then:*

$$(R_1R_2)^T(R_1R_2) = R_2^T R_1^T R_1 R_2 = R_2^T I_3 R_2 = I_3$$

and $\det(R_1R_2) = \det(R_1)\det(R_2) = 1 \cdot 1 = 1.$

2. ***Associativity**: Matrix multiplication is associative.*
3. ***Identity**: $I_3 \in SO(3)$ since $I_3^T I_3 = I_3$ and $\det(I_3) = 1$.*
4. ***Inverse**: For $R \in SO(3)$, $R^{-1} = R^T \in SO(3)$ because:*

$$(R^T)^T R^T = RR^T = I_3 \quad \textit{and} \quad \det(R^T) = \det(R) = 1$$

Key Differences from 2D Case

Property	**2D Rotations (SO(2))**	**3D Rotations (SO(3))**
Commutative	Yes (Abelian)	No (Non-abelian)
Dimension	1	3
Parameterization	Single angle θ	3 parameters (Euler angles: α, β, γ or axis-angle: $\hat{\mathbf{n}}, \theta$)
Manifold structure	Circle S^1	3-sphere with antipodes identified (Real projective space $\mathbb{RP}^3$)

Non-Commutativity Example in 3D

Rotations in 3D generally do not commute. Consider:

$$R_x(90^\circ) = \text{Rotation by } 90^\circ \text{ about x-axis}$$
$$R_y(90^\circ) = \text{Rotation by } 90^\circ \text{ about y-axis}$$

Then:

$$R_x(90^\circ)R_y(90^\circ) \neq R_y(90^\circ)R_x(90^\circ)$$

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

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

These are different matrices, demonstrating non-commutativity.

Applications in Machine Learning

Data Augmentation

Rotation groups provide natural symmetries for data augmentation:
- Image rotation (SO(2) for 2D images)
- 3D object rotation (SO(3) for point clouds, meshes)

Equivariant Neural Networks

Networks designed to respect rotational symmetry:
- **SO(2)-equivariant CNNs**: For 2D images
- **SO(3)-equivariant networks**: For 3D molecular data, point clouds
- Use group representation theory to design filters

Geometric Deep Learning

- SE(3) networks (combining SO(3) with translations)
- Spherical CNNs for data on spheres
- Steerable filters

Summary

- **2D rotations** form the abelian group SO(2) $\cong$ U(1) $\cong$ S^1
- **3D rotations** form the non-abelian group SO(3)
- Both are **Lie groups** (groups that are also smooth manifolds)
- SO(3) has dimension 3, while SO(2) has dimension 1
- The non-commutativity of 3D rotations has profound mathematical and physical consequences
- These groups are fundamental in machine learning for handling rotational symmetry

Theorem 1 *Both SO(2) and SO(3) are compact connected Lie groups. SO(2) is abelian, while SO(3) is simple and non-abelian.*

Appendix 3: $SO(2)$, $SO(3)$

The **Special Orthogonal groups** SO(2) and SO(3) are fundamental mathematical structures that describe rotations in two and three dimensions, respectively. They are essential in physics, computer graphics, robotics, and machine learning.

Definition 19 (Orthogonal Matrix) *An $n \times n$ real matrix R is **orthogonal** if:*

$$R^T R = R R^T = I_n$$

where R^T is the transpose of R and I_n is the $n \times n$ identity matrix.

Definition 20 (Determinant of Orthogonal Matrices) *For any orthogonal matrix R,* $\det(R) = \pm 1$.

SO(2): Rotations in Two Dimensions

Definition 21 (SO(2)) *The **Special Orthogonal group in 2 dimensions**, denoted SO(2), is the set of all 2×2 orthogonal matrices with determinant 1:*

$$SO(2) = \{R \in \mathbb{R}^{2\times 2} : R^T R = I_2,\ \det(R) = 1\}$$

Matrix Representation

Every element of SO(2) can be written as:

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{for some } \theta \in \mathbb{R}$$

Properties of SO(2)

Theorem 2 (Group Structure of SO(2)) *SO(2) forms a group under matrix multiplication:*

1. ***Closure**:* $R(\theta_1)R(\theta_2) = R(\theta_1 + \theta_2) \in SO(2)$
2. ***Associativity**: Matrix multiplication is associative*
3. ***Identity**:* $R(0) = I_2$
4. ***Inverse**:* $R(\theta)^{-1} = R(-\theta) = R(\theta)^T$

Theorem 3 (SO(2) is Abelian) *SO(2) is commutative:*

$$R(\theta_1)R(\theta_2) = R(\theta_1 + \theta_2) = R(\theta_2 + \theta_1) = R(\theta_2)R(\theta_1)$$

Algebraic Properties

Theorem 4 (Isomorphisms of SO(2)) *SO(2) is isomorphic to:*

1. *The **circle group*** $U(1) = \{e^{i\theta} : \theta \in \mathbb{R}\}$
2. *The **1-sphere*** $S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$
3. *The **real numbers modulo** 2π:* $\mathbb{R}/2\pi\mathbb{Z}$

SO(3): Rotations in Three Dimensions

Definition 22 (SO(3)) *The **Special Orthogonal group in 3 dimensions**, denoted SO(3), is the set of all 3×3 orthogonal matrices with determinant 1:*

$$SO(3) = \{R \in \mathbb{R}^{3\times 3} : R^T R = I_3,\ \det(R) = 1\}$$

Multiple Representations

1. Axis-Angle Representation

Every rotation in 3D can be described by an axis $\hat{\boldsymbol{n}} \in S^2$ (unit vector) and angle $\theta \in \mathbb{R}$:

$$R(\hat{\boldsymbol{n}}, \theta) = \exp(\theta[\hat{\boldsymbol{n}}]_\times)$$

where $[\hat{\boldsymbol{n}}]_\times$ is the cross-product matrix:

$$[\hat{\boldsymbol{n}}]_\times = \begin{pmatrix} 0 & -n_z & n_y \\ n_z & 0 & -n_x \\ -n_y & n_x & 0 \end{pmatrix}$$

2. Euler Angles

Three successive rotations about coordinate axes (e.g., ZYX convention):

$$R(\alpha, \beta, \gamma) = R_z(\alpha) R_y(\beta) R_x(\gamma)$$

3. Quaternions

Unit quaternions $q = (w, \boldsymbol{v})$ with $w^2 + \|\boldsymbol{v}\|^2 = 1$:

$$q = \cos(\theta/2) + \sin(\theta/2)(n_x i + n_y j + n_z k)$$

Properties of SO(3)

Theorem 5 (Group Structure of SO(3)) *SO(3) forms a group under matrix multiplication:*

1. ***Closure***: *Product of rotations is a rotation*
2. ***Associativity***: *Matrix multiplication is associative*
3. ***Identity***: $I_3 \in SO(3)$
4. ***Inverse***: $R^{-1} = R^T \in SO(3)$

Theorem 6 (SO(3) is Non-Abelian) *SO(3) is **not** commutative. For rotations about different axes:*

$$R_x(\alpha) R_y(\beta) \neq R_y(\beta) R_x(\alpha)$$

Applications

Physics

Computer Graphics and Robotics

- **SO(2)**: 2D image rotation, sprite animation
- **SO(3)**: 3D object orientation, robot arm kinematics

Machine Learning

- **SO(2)-equivariant networks**: For 2D images with rotational symmetry
- **SO(3)-equivariant networks**: For 3D point clouds, molecular data
- **Spherical CNNs**: Operating on S^2 using SO(3) representations

Computer Vision

- Camera calibration and pose estimation
- Structure from motion
- Image registration

Matrix Examples

SO(2) Example

Rotation by $\theta = \pi/3$ (60°):

$$R(\pi/3) = \begin{pmatrix} \cos(\pi/3) & -\sin(\pi/3) \\ \sin(\pi/3) & \cos(\pi/3) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

SO(3) Example

Rotation by $\pi/2$ about x-axis:

$$R_x(\pi/2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

Rotation by $\pi/2$ about y-axis:

$$R_y(\pi/2) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$$

Their non-commutativity:

$$R_x(\pi/2)R_y(\pi/2) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \neq R_y(\pi/2)R_x(\pi/2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$$

Summary

- **SO(2)** represents all rotations in the plane. It's a 1-dimensional abelian group isomorphic to the circle.
- **SO(3)** represents all rotations in 3D space. It's a 3-dimensional non-abelian group with rich structure.

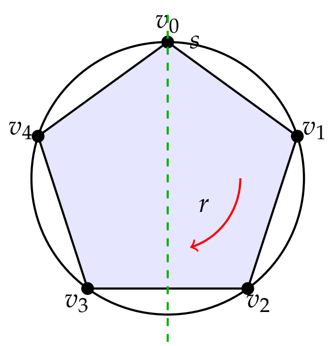
- The key difference is **commutativity**: SO(2) is abelian, while SO(3) is not.
- These groups are fundamental in physics and engineering for describing rotational symmetry.

Appendix 4: Symmetries of a Pentagon

We construct a group with 10 elements: the **dihedral group** D_5, which represents symmetries of a regular pentagon. The "triangle" operation $\triangle$ will represent function composition of these symmetries.

Let $G = \{e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4\}$ where:

- e = identity (do nothing)
- r = rotation by 72° ($2\pi/5$ radians) clockwise
- r^k = rotation by $72k$° (composition of k rotations)
- s = reflection across vertical axis (fixing vertex at top)
- sr^k = reflection followed by rotation



The "Triangle" Operation

Define $\triangle : G \times G \to G$ as function composition:

$$a \triangle b = b \circ a \quad \text{(apply } a \text{ first, then } b\text{)}$$

or equivalently in our notation: $a \triangle b$ means "do symmetry a, then symmetry b".

Group Axioms Verification

1. **Closure**: Composition of any two symmetries yields another symmetry of the pentagon.
2. **Associativity**: Function composition is always associative.
3. **Identity**: e is the identity: $e \triangle a = a \triangle e = a$ for all $a \in G$.
4. **Inverses**:
   - r^k has inverse r^{5-k} (since $r^5 = e$)
   - s is its own inverse: $s \triangle s = e$

- $(sr^k)^{-1} = sr^{5-k}$

Group Table for D_5

The following table defines $a \triangle b$ (read a from left column, b from top row):

$\triangle$	e	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
e	e	r	r^2	r^3	r^4	s	sr	sr^2	sr^3	sr^4
r	r	r^2	r^3	r^4	e	sr^4	s	sr	sr^2	sr^3
r^2	r^2	r^3	r^4	e	r	sr^3	sr^4	s	sr	sr^2
r^3	r^3	r^4	e	r	r^2	sr^2	sr^3	sr^4	s	sr
r^4	r^4	e	r	r^2	r^3	sr	sr^2	sr^3	sr^4	s
s	s	sr	sr^2	sr^3	sr^4	e	r	r^2	r^3	r^4
sr	sr	sr^2	sr^3	sr^4	s	r^4	e	r	r^2	r^3
sr^2	sr^2	sr^3	sr^4	s	sr	r^3	r^4	e	r	r^2
sr^3	sr^3	sr^4	s	sr	sr^2	r^2	r^3	r^4	e	r
sr^4	sr^4	s	sr	sr^2	sr^3	r	r^2	r^3	r^4	e

Key Properties

Non-Abelian

The group is **non-abelian** (not commutative). For example:

$$r \triangle s = sr^4 \quad \text{but} \quad s \triangle r = sr$$

Since $sr^4 \neq sr$, the operation doesn't commute.

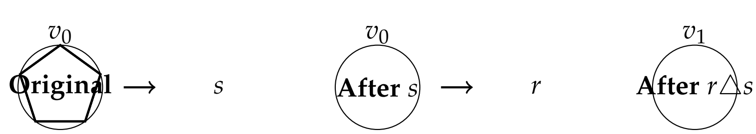
Subgroup Structure

- $\{e, r, r^2, r^3, r^4\}$ forms a **cyclic subgroup** of order 5 (rotations only)
- $\{e, s\}$ forms a subgroup of order 2
- $\{e, sr^k\}$ for any fixed k forms a subgroup of order 2

Visual Example of Operation

Consider $r \triangle s = sr^4$:

1. Start with pentagon in original position
2. Apply s: Reflect across vertical axis
3. Apply r: Rotate resulting figure by 72°
4. The net effect is equivalent to sr^4



Alternative Interpretation: Cyclic Group $\mathbb{Z}_{10}$

If we want an **abelian** group of order 10 with triangle as addition modulo 10:

Let $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ with operation:

$$a \triangle b = (a + b) \mod 10$$

$\triangle$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

This is the **cyclic group** $\mathbb{Z}_{10}$, which is abelian. (See Appendix 3 for a definition of cyclic group.)

Comparison

Property	**Dihedral** D_5	**Cyclic** $\mathbb{Z}_{10}$
Order	10	10
Abelian?	No	Yes
Operation	Function composition	Addition mod 10
Structure	Pentagonal symmetries	Integers modulo 10
Subgroups	More complex	Simple (all cyclic)

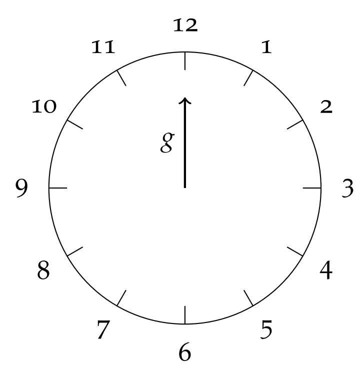
Conclusion

- The dihedral group D_5 provides a natural example of a 10-element group with geometric meaning.
- The "triangle" operation represents composition of symmetries.
- D_5 is non-abelian, illustrating that not all groups are commutative.
- Alternatively, $\mathbb{Z}_{10}$ gives an abelian group of order 10.
- Both are valid groups, demonstrating the diversity of group structures.

Appendix 3: Cyclic Groups

Intuitive Understanding

A **cyclic group** is the mathematical abstraction of "going around in circles" or "clock arithmetic." It represents the simplest possible group structure where every element can be generated from a single starting element.



$\mathbb{Z}_{12}$: Adding 1 hour repeatedly generates all hours

Formal Definition and Properties

Definition 23 (Cyclic Group) *A group $(G, *)$ is **cyclic** if there exists an element $g \in G$ such that:*

$$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

where:

- $g^0 = e$ *(the identity element)*
- $g^n = \underbrace{g * g * \cdots * g}_{n \text{ times}}$ *for* $n > 0$
- $g^{-n} = (g^{-1})^n = \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{n \text{ times}}$ *for* $n > 0$

*The element g is called a **generator** of G. We write $G = \langle g \rangle$.*

Types of Cyclic Groups

1. **Finite Cyclic Groups**: Have a finite number of elements. Denoted $\mathbb{Z}_n$ or C_n.
2. **Infinite Cyclic Groups**: Have infinitely many elements. The only example is $\mathbb{Z}$ (integers under addition).

Examples of Cyclic Groups

Example 1: Integers Modulo n ($\mathbb{Z}_n$)

For any positive integer n, the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ with addition modulo n forms a cyclic group.

Example 8 ($\mathbb{Z}_6$) *Let $G = \{0, 1, 2, 3, 4, 5\}$ with addition modulo 6.*

- *Generator:* 1 *generates all elements:*

$$\begin{aligned} 1 &\to 1 \\ 1+1 &= 2 \\ 1+1+1 &= 3 \\ 1+1+1+1 &= 4 \\ 1+1+1+1+1 &= 5 \\ 1+1+1+1+1+1 &= 0 \ (\textit{mod } 6) \end{aligned}$$

- *Also generator:* 5 *(since* $5 \equiv -1 \mod 6$*)*
- *Not generator:* 2 *only generates* $\{0, 2, 4\}$ *(subgroup of order 3)*
- *Order:* $|G| = 6$