LIE THEORY

TRISTAN LIU, ARPIT MITTAL, AND MARK TAKKEN

Contents

Introduction

Lie groups were introduced by Sophus Lie to model continuous symmetries of differential equations. Lie groups are groups that are simultaneously smooth manifolds. These groups have group operations of multiplication and inversion which are smooth maps. Due to this property, it is meaningful and useful to additionally study the tangent space of a Lie group at its identity, which is called the Lie algebra. Main examples of a Lie group are matrix groups, such as the group of invertible matrices over a field such as $\mathbb{C}$, or the group of orthogonal matrices. In this paper, we will primarily consider matrix groups. To give some insight for this choice, it turns out that any compact Lie group is isomorphic to some matrix group and that every finite-dimensional Lie group has a finite-dimensional Lie algebra that is a matrix algebra. In this sense, matrix groups capture many important parts of Lie Theory while being more accessible. Lie groups naturally arise when considering spatial symmetries, which frequently appear in areas of quantum theory and computer vision/graphics, for example.

In section 1, we rigorously develop the notions of matrix norms and Banach spaces which we will be using throughout the paper. In section 2, we introduce matrix groups and describe some of their algebraic and topological properties. In section 3, we introduce the matrix exponential and logarithm, which are crucial for the Lie group-Lie algebra correspondence, and described how to practically calculate them. In section 4, we introduce Lie algebras and the exponential and logarithmic maps between the Lie algebra and the Lie group. We conclude this section with an interesting theorem pertaining to continuous maps between Lie groups. In section 5, we introduce some representation theory which is then utilized in the subsequent section 6 on the applications of Lie groups and representation theory to quantum theory. Finally, in section 7 we discuss applications to object tracking in computer vision.

Date: Spring 2022.

We will assume knowledge of some group theory, linear algebra, and analysis (at the level of a first course). Any results cited should be well-known and can be found in any standard introductory text.

1. Matrix norms and Banach spaces

Definition 1.1. A metric space is a a set X with a distance function $d : X \times X \to \mathbb{R}$ such that for all $x, y, z \in X$

- $d(x, y) \geq 0$ with $d(x, y) = 0$ if and only if $x = y$ (positive definite),
- $d(x, y) = d(y, x)$ (symmetry),
- and $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

Definition 1.2. A sequence x_n in a metric space (X, d) converges to x if given $\varepsilon > 0$, there exists N such that for all $n > N$, $d(x_n, x) < \varepsilon$.

Definition 1.3. A sequence x_n in a metric space (X, d) is a Cauchy sequence if given $\varepsilon > 0$, there exists N such that for all $n, m > N$, $d(x_n, x_m) < \varepsilon$.

Metric spaces allow us to generalize the notion of convergence, which lets us prove generalizations of many results that may be familiar from real analysis.

Definition 1.4. A metric space is complete if all Cauchy sequences are convergent.

Example. $\mathbb{R}^n$ and $\mathbb{C}^n$ are complete under the standard Euclidean metric.

Definition 1.5. A norm on a real/complex vector space is a real valued function $|| \cdot ||$ which satisfies the following properties. For any vectors x, y and scalar α, we have

- $||x|| \geq 0$ with $||x|| = 0$ if and only if $x = 0$,
- $||\alpha x|| = |\alpha| \, ||x||$,
- and $||x + y|| \leq ||x|| + ||y||$.

Proposition 1.6. *A normed vector space is a metric space under the metric* $d(x, y) = ||x - y||$.

Proof. The properties of a metric space are all easily inherited from the properties of a norm.

- We have $||x - y|| \geq 0$ with $||x - y|| = 0$ if and only if $x - y = 0$, which is equivalent to $x = y$.
- We have $||x - y|| = | - 1| \, ||y - x|| = ||y - x||$.
- We have $||x - z|| \leq ||x - y|| + ||y - z||$. □

We will often implicitly consider a normed vector space as a metric space under this metric.

Remark 1.7. We will use $\mathbb{K}$ to denote either $\mathbb{R}$ or $\mathbb{C}$.

Definition 1.8. We let $M_n(\mathbb{K})$ denote the set of square $n \times n$ matrices over $\mathbb{K}$.

Definition 1.9. The operator norm of an $n \times n$ matrix is

$$||A|| = \max(\{\frac{||Ax||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}).$$

Note that

$$\frac{||A(\alpha x)||}{||\alpha x||} = \frac{||Ax||}{||x||}$$

for any scalar α, so we can assume vectors are normalized to have magnitude 1 and equivalently define

$$||A|| = \max(\{\frac{||Ax||}{||x||} : x \in \mathbb{K}^n, |x| = 1\}.$$

This norm is well defined because $\{x : |x| = 1\}$, as a compact set, will have a compact image under the continuous function $\frac{||Ax||}{||x||}$, and thus will have a maximum value.

Proposition 1.10. *The operator norm is a norm.*

Proof. By definition of $||A||$, it is the maximum of nonnegative numbers, and thus must be nonnegative. It is 0 if and only if $||Ax|| = 0$ for all x, which would imply $A = 0$.

For a complex scalar α,

$$||\alpha A|| = \max(\{\frac{||\alpha Ax||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) = |\alpha| \max(\{\frac{||Ax||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) = |\alpha| |\, |A||$$

as desired.

Lastly, $||A + B|| = \max(\{\frac{||Ax+Bx||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) \leq \max(\{\frac{||Ax||+||Bx||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) \leq \max(\{\frac{||Ax||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) + \max(\{\frac{||Bx||}{||x||} : x \in \mathbb{K}^n, x \neq 0\}) = ||A|| + ||B||$ so the operator norm satisfies the triangle inequality. □

Definition 1.11. The Hilbert Schmidt norm of an $n \times n$ matrix is

$$||A|| = \sqrt{\sum_{1 \leq i,j \leq n} |a_{ij}|^2}.$$

Proposition 1.12. *The Hilbert Schmidt norm is a norm.*

Proof. As $||A||$ is the sum of nonnegative numbers, we have $||A|| \geq 0$ and $||A|| = 0$ if and only if all the entries of A are 0, namely, if $A = 0$.

It is also clear that

$$||\alpha A|| = \sqrt{\sum_{1 \leq i,j \leq n} |\alpha a_{ij}|^2} = \sqrt{|\alpha^2| \sum_{1 \leq i,j \leq n} |a_{ij}|^2} = |\alpha| \sqrt{\sum_{1 \leq i,j \leq n} |a_{ij}|^2} = |\alpha|\, ||A||.$$

Lastly, we check the triangle inequality. We have the bound

$$||A + B|| = \sqrt{\sum_{1 \leq i,j \leq n} |a_{ij} + b_{ij}|^2} \leq$$

$$\sqrt{\sum_{1 \leq i,j \leq n} (|a_{ij}| + |b_{ij}|)^2} =$$

$$\sqrt{\sum_{1 \leq i,j \leq n} |a_{ij}|^2 + 2 \sum_{1 \leq i,j \leq n} |a_{ij}||b_{ij}| + \sum_{1 \leq i,j \leq n} |b_{ij}|^2} \leq$$

$$\sqrt{\sum_{1 \leq i,j \leq n} |a_{ij}|^2 + 2(\sum_{1 \leq i,j \leq n} |a_{ij}|^2)^{1/2}(\sum_{1 \leq i,j \leq n} |b_{ij}|^2)^{1/2} + \sum_{1 \leq i,j \leq n} |b_{ij}|^2} = \sqrt{\sum_{1 \leq i,j \leq n} |a_{ij}|^2} + \sqrt{\sum_{1 \leq i,j \leq n} |b_{ij}|^2} =$$

$$||A|| + ||B||$$

by Cauchy-Schwarz. □

Theorem 1.13. *If we have two norms $||\cdot||$ and $||\cdot||'$ over a finite dimensional real/complex vector space V, they define equivalent topologies. In particular, there exist constants $A, B > 0$ such that $A||v||' \leq ||v|| \leq B||v'||$.*

The proof of this is too involved to include, so we refer you to Keith Conrad's paper [9] for details.

Remark 1.14. This gives us a bound by a scalar multiple between any matrix norms. This means if $||x_n - x||$ converges to 0 under one norm, it does under every norm. Thus a sequence x_n that converges to x under one matrix norm also converges to the same thing under any other norm. This allows us to talk about convergence of matrix sequences by using any norm we like, as all of them are effectively equivalent.

Definition 1.15. A Banach space is a complete normed vector space.

Example. $M_n(\mathbb{K})$ is a Banach space because it is a normed vector space that is complete (as it is isomorphic to the complete space $\mathbb{K}^{n^2}$ under the Hilbert Schmidt norm).

Definition 1.16. Let B be a metric space. A sequence of functions $f_n : A \to B$ converges pointwise to $f : A \to B$ if for all $a \in A$, the sequence $f_n(a)$ converges. A sequence converges uniformly to f if for all $\varepsilon > 0$, there exists N such that for all $n > N$ and $a \in A$,

$$d(f_n(a), f(a)) < \varepsilon.$$

Uniform convergence is a stronger condition than pointwise convergence because given ε, we use the same N independent of $a \in A$.

Definition 1.17. Let $b(X, Y)$ be the vector space of bounded functions from a set X to a Banach space Y. We can define the sup norm on this space as $||f|| = \sup_{x \in X} ||f(x)||$.

Remark 1.18. Convergence under the sup norm is equivalent to absolute convergence.

Proposition 1.19. *The space $b(X, Y)$ under the sup norm is a Banach space*

Proof. We verify $b(X, Y)$ is a vector space. Suppose f and g are bounded functions, say with $||f|| = N_1$ and $||g|| = N_2$. Then for all $x \in X$, $||(f+g)(x)|| = ||f(x)+g(x)|| \leq ||f(x)||+||g(x)|| \leq N_1 + N_2$ by the triangle inequality for the norm on Y. Furthermore the image of αf is just α times the image of f. Because the f is bounded, αf must then also be bounded, in fact with supremum $|\alpha|||f||$

This also shows that the sup norm satisfies the triangle inequality and that $||\alpha f|| = |\alpha|\,||f||$. By definition it is clear $||f|| = 0$ if and only if $f = 0$. Thus our sup norm is in fact a norm.

Suppose f_n is a Cauchy sequence under the sup norm. Then, for any fixed $x \in X$, $f_n(x)$ is a Cauchy sequence in Y and must thus converge. For each x, we define $f(x)$ to be the limit of the sequence $f_n(x)$. We then have, by definition, that f_n will converge pointwise to f. We now show it converges uniformly. Let $\varepsilon > 0$. Choose N such that for any $m, n > N$, $||f_m - f_n|| < \frac{\varepsilon}{2}$. We now show, for $n > N$ and for arbitrary $x \in X$, $||f_n(x) - f(x)|| < \varepsilon$. By pointwise convergence, we can find $m > N$ such that $||f_m(x) - f(x)|| < \frac{\varepsilon}{2}$. Thus,

$$||f_n(x) - f(x)|| \leq ||f_n(x) - f_m(x)|| + ||f_m(x) - f(x)|| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

as desired. Thus f_n converges to f under the sup norm, so $b(X, Y)$ is complete and a Banach space. □

Definition 1.20. Let A and B be metric spaces. A function $f : A \to B$ is continuous at $a \in A$ if for any $\varepsilon > 0$, there exists $\delta > 0$ such that if $d(a, x) < \delta$, then $d(f(a), f(x)) < \varepsilon$.

Example. Polynomials in $\mathbb{C}^n$ are continuous.

Example. Matrices under the Hilbert Schmidt norm are isomorphic to $\mathbb{C}^n$, and thus functions that are polynomial in terms of the matrix entries are continuous. Namely, matrix products, transposes, determinants, and traces, are continuous.

Theorem 1.21. *If a sequence of continuous functions $f_n : X \to Y$ converges uniformly to $f : X \to Y$, then f is continuous.*

Proof. Let $\varepsilon > 0$. Consider an arbitrary $x \in X$. We show f is continuous at x. By uniform convergence, we can find N such that $d(f_N(t), f(t)) < \frac{\varepsilon}{3}$ for all $t \in X$. We have f_n is continuous at x, so let δ be such that if $|x - y| < \delta$, $|f_n(x) - f_n(y)| < \frac{\varepsilon}{3}$.

If $|x - y| < \delta$,

$$|f(x) - f(y)| < |f(x) - f_N(x)| + |f_N(x) - f_N(y)| + |f_N(y) - f(y)| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$$

as desired. Thus f is continuous. □

Definition 1.22. In a normed space, a series $\sum_{n=1}^{\infty} a_n$ is convergent if its partial sums converge and is absolutely convergent if $\sum_{n=1}^{\infty} ||a_n||$ converges.

Theorem 1.23. *In a Banach space, every absolutely convergent series is convergent.*

Proof. Let $\sum_{k=1}^{\infty} ||a_k||$ be convergent. We show the partial sums $s_n = \sum_{k=1}^{n} a_k$ are Cauchy. Let $\varepsilon > 0$. Because $\sum_{k=1}^{\infty} ||a_k||$ is convergent, we can find some N such that $\sum_{k=N+1}^{\infty} ||a_k|| < \varepsilon$. For any $m \geq n > N$, we have

$$||s_m - s_n|| = ||\sum_{k=1}^{m} a_k - \sum_{k=1}^{n} a_k|| = ||\sum_{k=n+1}^{m} a_k|| \leq \sum_{k=n+1}^{m} ||a_k|| \leq \sum_{k=N+1}^{\infty} ||a_k|| < \varepsilon$$

by the triangle inequality. Thus, the partial sums are Cauchy and the series converges. □

Theorem 1.24 (Weierstrass M-test)**.** *Let f_n be a sequence of functions from a set X to a Banach space Y. If there exists a sequence M_n such that $||f_n(x)|| \leq M_n$ for all x and n and $\sum_{n=1}^{\infty} M_n$ converges, then $\sum_{n=1}^{\infty} f_n(x)$ converges absolutely and uniformly on the set.*

Proof. We can think of the functions as being in $b(X, Y)$. We have $\sum_{n=1}^{\infty} ||f_n(x)|| < \sum_{n=1}^{\infty} M_n$ which converges, so $\sum_{n=1}^{\infty} f_n(x)$ converges absolutely under the sup norm. Thus, it must converge under the sup norm, which demonstrates uniform convergence. □

2. Matrix Groups

Definition 2.1. The general linear group, $\mathrm{GL}_n(\mathbb{K})$ is the group of all matrices in $M_n(\mathbb{K})$ with nonzero determinant under matrix multiplication.

Remark 2.2. If $A \in \mathrm{GL}_n(\mathbb{K})$, then we can consider

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

to be a member of $\mathrm{GL}_n(\mathbb{K})$ as well.

Remark 2.3. Alternatively, $\mathrm{GL}_n(\mathbb{K})$ is the group of all invertible matrices in $M_n(\mathbb{K})$ under matrix multiplication.

Proposition 2.4. *The general linear groups are groups.*

Proof. We can straightforwardly check all the group axioms. The product of two invertible matrices in $\mathbb{K}$ is an invertible matrix in $\mathbb{K}$. Matrix multiplication is associative, the identity matrix is an identity for matrix multiplication, and all matrices with nonzero determinant are invertible. ☐

Definition 2.5. A matrix group is a closed subgroup of $\mathrm{GL}_n(\mathbb{C})$. In other words, any convergent sequence in the matrix group converges to an element of the matrix group or a noninvertible matrix.

Example. $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{GL}_n(\mathbb{R})$ are matrix groups. They are both clearly subgroups of $\mathrm{GL}_n(\mathbb{C})$ and any sequence $A_m \in \mathrm{GL}_n(\mathbb{K})$ converges to a matrix in $M_n(\mathbb{K})$, and thus must converge to a matrix in $GL_n(\mathbb{K})$ or a noninvertible matrix.

Definition 2.6. The special linear group $\mathrm{SL}_n(\mathbb{K})$ is the group of all matrices in $M_n(\mathbb{K})$ that have determinant 1.

Proposition 2.7. *The special linear groups are matrix groups.*

Proof. We first check the special linear groups are subgroups of $\mathrm{GL}_n(\mathbb{C})$. They are clearly a subset, and closure under multiplication and inverses both follow immediately from the multiplicativity of the determinant and the fact the products and inverses of matrices in $\mathbb{K}$ are in $\mathbb{K}$.

If a sequence of matrices with determinant 1 converges, it must converge to a matrix with determinant 1 by the continuity of the determinant. Therefore the special linear groups are closed.

We have shown that the special linear groups, as desired, are matrix groups. ☐

Proposition 2.8. *If $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$, then $GL_n(\mathbb{K}) \subseteq M_n(\mathbb{K})$ is an open subset, and $SL_n(\mathbb{K}) \subseteq M_n(\mathbb{K})$ is a closed subset.*

Proof. The determinant $\det : M_n(\mathbb{K}) \to \mathbb{K}$ is a continuous function. Then

$$\mathrm{GL}_n(\mathbb{K}) = M_n(\mathbb{K}) \setminus \det^{-1}\{0\}$$

is an open set because $\{0\}$ is closed in $\mathbb{K}$. Similarly, we have that

$$\mathrm{SL}_n(\mathbb{K}) = \det^{-1}\{1\} \subseteq \mathrm{GL}_n(\mathbb{K})$$

is closed because $\{1\}$ is closed in $\mathbb{K}$. ☐

Definition 2.9. The standard inner product on $\mathbb{C}^n$ is given by

$$\langle x, y\rangle = \sum_{i=1}^{n} \bar{x}_i y_i.$$

The natural extension of the dot product from the reals to the complex numbers given by $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$ does not work, as, if $\langle u, u\rangle > 0$, then

$$\langle iu, iu\rangle = i^2\langle u, u\rangle = -\langle u, u\rangle < 0,$$

contradicting positive definiteness.

Definition 2.10. The conjugate transpose (also called the adjoint or Hermitian conjugate) of a matrix A is $A^* = \overline{A^T}$.

Definition 2.11. A unitary matrix is a matrix $U \in M_n(\mathbb{C})$ such that $U^*U = I$

Theorem 2.12. *The following conditions are equivalent:*

- *$U^*U = I$*
- *The columns of U form an orthonormal set*
- *U preserves the inner product (ie for all x, y, $\langle x, y\rangle = \langle Ux, Uy\rangle$)*

Proof. If $U^*U = I$, then, for all i, j, we have that $U^*_{i*} \cdot U_{*j} = \delta_{ij}$ where δ_{ij} is the Kronecker delta which equals 1 if $i = j$ and 0 otherwise.

Because the rows of the transpose are the same as the columns of the matrix and that the product with the conjugate transpose is the same as the inner product, this is equivalent to saying that $U_{*i} \cdot U_{*j} = \delta_{ij}$ which is precisely the definition of an orthonormal set.

If $U^*U = I$, we have $\langle Ux, Uy\rangle = (Ux)^*Uy = x^*U^*Uy = x^*y = \langle x, y\rangle$.

Conversely, if $\langle Ux, Uy\rangle = \langle x, y\rangle$, we have $\langle Ue_i, Ue_j\rangle = \langle e_i, e_j\rangle = \delta_{ij}$ for all i, j. Thus $e_i^*U^*Ue_j = \delta_{ij}$ for all i, j. Multiplying out $e_i^*Me_j$ for arbitrary M gives M_{ij}. Thus, $(U^*U)_{ij} = \delta_{ij}$ for all i, j, so $U^*U = I$.

□

Proposition 2.13. *If U is unitary, $|\det(U)| = 1$.*

Proof. We have $\det(U^*) = \det(\overline{U^T}) = \det(\overline{U})$. Complex conjugation distributes over the operations of addition, subtraction, multiplication, and division, and the determinant is a polynomial with real coefficients in terms of its entries, so $\det(U^*) = \det(\overline{U}) = \overline{\det(U)}$.

Thus,

$$1 = \det(I) = \det(U^*U) = \det(U^*)\det(U) = \overline{\det(U)}\det(U) = |\det(U)|^2.$$

So $|\det(U)| = 1$ as desired. □

Definition 2.14. An orthogonal matrix is a matrix $A \in M_n(\mathbb{R})$ with columns that form an orthonormal set.

They are the restriction of Unitary matrices to real matrices. Accordingly, equivalent conditions for A being orthogonal include $AA^T = I$ and A preserving the inner product on $\mathbb{R}^n$.

Definition 2.15. The Unitary group $U(n)$ is made of all the unitary $n \times n$ matrices. The special unitary group $SU(n)$is the subgroup of $U(n)$ with matrices of determinant 1. Similarly, the orthogonal group $O(n)$ is made of all $n \times n$ orthogonal matrices and the special orthogonal Group $SO(n)$ is the subgroup of $O(n)$ with matrices of determinant 1.

Remark 2.16. The orthogonal group can be thought of as the group of rotations and reflections in $\mathbb{R}^n$ while the special orthogonal group can be thought of as encoding just rotations.

Proposition 2.17. *$U(n), SU(n), O(n)$, and $SO(n)$ are matrix groups.*

Proof. Unitary matrices are clearly a subset of $GL_n(\mathbb{C})$ as $|\det(U)| = 1$ for all $U \in U(n)$. We check they are closed under matrix multiplication and inverses. Let U_1 and U_2 be unitary. Then

$$(U_1U_2)^*U_1U_2 = U_2^*U_1^*U_1U_2 = U_2^*(U_1^*U_1)U_2 = U_2^*U_2 = I,$$

so U_1U_2 is unitary as desired. Similarly, $(U^*)^*U^* = UU^* = I$, so $U^{-1} = U^*$ is unitary.

Closure easily follows from the continuity of the function M^*M, as any sequence of matrices that satisfy $M^*M = I$ must limit to a matrix that also satisfies $M^*M = I$.

The proofs for $SU(n)$, $O(n)$, and $SO(n)$ are easily checked and essentially identical to those for $SL_n(\mathbb{K})$ and $GL_n(\mathbb{R})$ and hence are omitted. □

2.1. Semidirect product.

Definition 2.18. Let G be a group with $H \leq G$ and $N \triangleleft G$. Then we say G is a *semidirect product* of H and N if $G = HN$ and $H \cap N = \{I\}$, which is denoted by $G = H \ltimes N$.

Definition 2.19. We define the *n-dimensional affine group* over $\mathbb{K}$ to be

$$\mathrm{Aff}_n(\mathbb{K}) = \left\{ \begin{pmatrix} A & \mathbf{t} \\ 0 & 1 \end{pmatrix} \mid A \in \mathrm{GL}_n(\mathbb{K}), \mathbf{t} \in \mathbb{K}^n \right\} \leq GL_{n+1}(\mathbb{K}).$$

Definition 2.20. We define the *translational subgroup* of $\mathrm{Aff}_n(\mathbb{K})$ to be

$$\mathrm{Trans}_n(\mathbb{K}) = \left\{ \begin{pmatrix} I_n & \mathbf{t} \\ 0 & 1 \end{pmatrix} \mid \mathbf{t} \in \mathbb{K}^n \right\} \leq \mathrm{GL}_{n+1}(\mathbb{K}).$$

Proposition 2.21. *$Trans_n(\mathbb{K})$ is a normal subgroup of $Aff_n(\mathbb{K})$ and $Aff_n(\mathbb{K})$ can be expressed as the semidirect product*

$$Aff_n(\mathbb{K}) = GL_n(\mathbb{K}) \ltimes Trans_n(\mathbb{K}).$$

Proof. Given $\begin{pmatrix} I & \mathbf{t} \\ 0 & 1 \end{pmatrix} \in \mathrm{Trans}_n(\mathbb{K})$ and any $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Trans}_n(\mathbb{K})$, we see that the conjugation

$$\begin{aligned} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I & \mathbf{t} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} A & A\mathbf{t} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} I & A\mathbf{t} \\ 0 & 1 \end{pmatrix} \end{aligned}$$

lies in $\mathrm{Trans}_n(\mathbb{K})$. Thus, $\mathrm{Trans}_n(\mathbb{K}) \triangleleft \mathrm{Aff}_n(\mathbb{K})$. Furthermore,

$$\left\{ \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I & \mathbf{t} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & A\mathbf{t} \\ 0 & 1 \end{pmatrix} : A \in \mathrm{GL}_n(\mathbb{K}), \mathbf{t} \in \mathrm{Trans}_n(\mathbb{K}) \right\}$$

is in bijection with $\mathrm{Aff}_n(\mathbb{K})$, since A is an invertible matrix. Lastly, we have

$$\mathrm{Trans}_n(\mathbb{K}) \cap \mathrm{GL}_n(\mathbb{K}) = 0$$

because non-trivial translations do not fix $\mathbf{0}$, while all elements of $\mathrm{GL}_n(\mathbb{K})$ do. □

Definition 2.22. An *isometry* is a function $f : \mathbb{R}^n \to \mathbb{R}^n$ such that $|f(\mathbf{a} - \mathbf{b})| = |\mathbf{a} - \mathbf{b}|$ for all vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$.

Definition 2.23. The group of isometries in $\mathbb{R}^n$ is denoted as

$$\mathrm{Isom}_n(\mathbb{R}) = \{f : \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ is an isometry}\}.$$

Proposition 2.24. *$Trans_n(\mathbb{R})$ is a normal subgroup of $Isom_n(\mathbb{R})$ and $Isom_n(\mathbb{R})$ can be expressed as the semidirect product*

$$Isom_n(\mathbb{R}) = O(n) \ltimes Trans_n(\mathbb{R}).$$

This is proven in the exact same way as the preceding proposition.

3. Matrix Exponential

Definition 3.1. Let M be a square matrix. We define e^M, also denoted $\exp(M)$, by the power series

$$e^M = \sum_{n=0}^{\infty} \frac{M^n}{n!}.$$

In order for this definition to make sense, we must check that e^M in fact converges, and consequently that this operation is well defined.

Lemma 3.2 (Submultiplicative matrix norm). *For any $n \times n$ matrices A, B, $||AB|| \leq ||A||||B||$.*

Proof (for operator norm). By definition of operator norm, we have $||A||\,||x|| \leq ||Ax||$. Thus, for all x, we have

$$||ABx|| \leq ||A||\,||Bx|| \leq ||A||\,||B||\,||x||.$$

We then have $||AB|| \leq ||A||\,||B||$ as desired. □

Proposition 3.3. *The series for e^M converges for all M. Furthermore e^M is continuous.*

Proof. We have, under the operator norm, that $||M^n|| \leq ||M||^n$ for $n \geq 0$ (we use our lemma for $n \geq 1$ and note $||M^0|| = 1 = ||M||^0$), so

$$\sum_{n=0}^{\infty} ||\frac{M^n}{n!}|| \leq \sum_{n=0}^{\infty} \frac{||M||^n}{n!} = e^{||M||}.$$

Thus, $e^M = \sum_{n=0}^{\infty} \frac{M^n}{n!}$ converges absolutely for any M, and must thus converge for any M as desired. Furthermore, these bounds satisfy the conditions of the Weierstrass M-test, so the series converges uniformly. Each of the partial sums is a finite sum of matrix products, and hence continuous. By uniform convergence, the limit is also continuous. □

Proposition 3.4. *If A and B commute, $e^{A+B} = e^A e^B$.*

Proof. By definition, $e^A e^B = (\sum_{n=0}^{\infty} \frac{1}{n!} A^n)(\sum_{n=0}^{\infty} \frac{1}{n!} B^n)$. We expand the product (which is allowed by absolute convergence) to get

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{k!(n-k)!} A^k B^{n-k} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k}.$$

By the binomial theorem (which we can use because A and B commute), this just equals $\sum_{n=0}^{\infty} \frac{1}{n!}(A+B)^n = e^{A+B}$ as desired. □

Proposition 3.5. *The derivative of e^{At} is Ae^{At}*

Proof. We have $e^{At} = \sum_{n=0}^{\infty} \frac{A^n}{n!} t^n$. Because it is a power series, we can differentiate term by term, so $\frac{d}{dt} e^{At} = \sum_{n=1}^{\infty} n \frac{A^n}{n!} t^{n-1}$

□

Theorem 3.6. *The system of differential equations given by $\frac{d}{dt} y = Ay$ with initial condition $y(0) = y_0$ where A is a constant matrix has the unique solution*

$$y(t) = e^{At} y_0.$$

Proof. By the Picard-Lindelöf theorem, there exists a unique solution to the differential equation.

We have $\frac{d}{dt} e^{At} y_0 = Ae^{At} y_0$ and $e^{A \cdot 0} y_0 = y_0$, so $e^{At} y_0$ must be our unique solution. □

Proposition 3.7. *For invertible A,*

$$e^{ABA^{-1}} = Ae^B A^{-1}$$

Proof. We have

$$e^{ABA^{-1}} = \sum_{n=0}^{\infty} \frac{1}{n!}(ABA^{-1})^n = \sum_{n=0}^{\infty} \frac{1}{n!} AB^n A^{-1} = A\left(\sum_{n=0}^{\infty} \frac{1}{n!} B^n\right) A^{-1} = Ae^B A^{-1},$$

as desired. □

Lemma 3.8. *Diagonalizable matrices are dense in $M_n(\mathbb{C})$.*

Proof. The coefficients of the characteristic polynomial $p(\lambda) = c_n\lambda^n + \cdots + c_1\lambda + c_0$ of a matrix are polynomials in the entries of the matrix. Now, letting the roots of the polynomial be $r_1, r_2, \ldots, r_n$, we define its discriminant as

$$D(p) = c_n^{2n-2} \prod_{i<j} (r_i - r_j)^2.$$

The product $\prod_{i<j}(r_i - r_j)^2$ is a symmetric polynomial in terms of the roots, so by the Fundamental Theorem of Symmetric Polynomials, it can be expressed as a polynomial in terms of the elementary symmetric polynomials e_k, where

$$e_k(r_1, r_2, \ldots, r_n) = \sum_{1 \le j_1 < \cdots < j_k \le n} r_{j_1} r_{j_2} \ldots r_{j_k}.$$

The degree of this polynomial is equal to $2(n-1)$, since the maximum power of each root r_i is equal to $2(n-1)$. Furthermore, by Vieta's formulas, we know that $e_k = (-1)^k \frac{c_{n-k}}{c_n}$; therefore, by multiplying the polynomial by c_n^{2n-2}—yielding the discriminant,—we obtain a polynomial in terms of the coefficients c_i, which is also a polynomial in terms of the entries of the matrix in question. Now, the discriminant is equal to zero if and only if all of the roots of the characteristic polynomial are distinct, so if the discriminant is nonzero, then the matrix is diagonalizable. Polynomials have roots only at isolated points, so there exists no open subset of the entries of the matrix for which the matrix is always not diagonalizable. That is, the diagonalizable matrices are dense. □

This lemma is very useful as it allows us to prove any continuous property of matrices by proving it for diagonalizable matrices.

Theorem 3.9 (Cayley-Hamilton)**.** *If $p(\lambda)$ is the characteristic polynomial of M, $p(M) = 0$.*

Proof. Let $M = PDP^{-1}$ be a diagonalizable matrix with characteristic polynomial $p(\lambda) = \sum_{k=0}^{n} c_k\lambda^k$. Then

$$p(M) = \sum_{k=0}^{n} c_k M^k = \sum_{k=0}^{n} c_k PD^k P^{-1} = Pp(D)P^{-1}.$$

Let $D = \text{diag}(\lambda_1, \lambda_2, \cdots, \lambda_m)$. Then

$$\begin{aligned} p(D) &= \sum_{k=0}^{n} c_k D^k \\ &= \sum_{k=0}^{n} c_k \text{diag}(\lambda_1^k, \lambda_2^k, \cdots, \lambda_k^k) \\ &= \text{diag}(\sum_{k=0}^{n} c_k \lambda_1^k, \sum_{k=0}^{n} c_k \lambda_2^k, \cdots, \sum_{k=0}^{n} c_k \lambda_m^k) = \text{diag}(p(\lambda_1), p(\lambda_2), \cdots, p(\lambda_m)) \\ &= 0, \end{aligned}$$

as $p(\lambda_i) = 0$ for all i.

Thus, Cayley-Hamilton holds for any diagonalizable matrix. As diagonalizable matrices are dense and $p(M)$ continuously varies, $p(M)$ must be 0 for all matrices. □

We now turn our attention to actually computing e^M for a given matrix M. We split this into three cases: where M is diagonalizable, where M is nilpotent, and where M is neither.

First, note that it is very easy to take the exponential of a diagonal matrix. If $A = \text{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$, then

$$\begin{aligned} e^A &= \sum_{k=0}^{\infty} \frac{A^k}{k!} \\ &= \sum_{k=0}^{\infty} \text{diag}\left(\frac{\lambda_1^k}{k!}, \frac{\lambda_2^k}{k!}, \cdots, \frac{\lambda_n^k}{k!}\right) \\ &= \text{diag}\left(\sum_{k=0}^{\infty} \frac{\lambda_1^k}{k!}, \sum_{k=0}^{\infty} \frac{\lambda_2^k}{k!}, \cdots, \sum_{k=0}^{\infty} \frac{\lambda_n^k}{k!}\right) \\ &= \text{diag}\left(e^{\lambda_1}, e^{\lambda_2}, \cdots, e^{\lambda_n}\right). \end{aligned}$$

Thus, for a diagonalizable matrix $M = PDP^{-1}$, we can compute $e^M = Pe^D P^{-1}$.

For a nilpotent matrix N, $N^k = 0$ for some k so $e^N = \sum_{m=0}^{k-1} \frac{1}{m!} N^m$, which is a finite sum that can be easily computed, as matrix multiplication is fast.[1]

All other matrices can be reduced to these two cases.

Lemma 3.10. *All strictly upper triangular matrices are nilpotent. In particular, if $M \in M_n(\mathbb{C})$ is strictly upper triangular, then $M^n = 0$.*

Proof. Let $e_1, \cdots, e_n$ be the standard basis of $\mathbb{C}^n$ and let U_i be the span of the first i basis vectors. Interpreting M as a linear transformation, e_i is mapped into U_{i-1} for all i. Thus, $MU_i \subseteq U_{i-1}$. Repeated application yields $M^n U_n = U_0$. As U_n is the whole of $\mathbb{C}^n$ and U_0 is the zero vector, we have that M^n maps every vector to the zero vector, and consequently $M^n = 0$ as desired.

Alternatively, the characteristic polynomial is t^n, so by the Cayley Hamilton theorem, $M^n = 0$. □

Proposition 3.11 (Jordan-Chevalley decomposition)**.** *Any matrix M can be decomposed into $M = S + N$ where S is diagonalizable, N is nilpotent, and S and N commute.*

[1] The Strassen algorithm runs in $O(n^{\log_2 7})$ time

Proof. Let $M = PJP^{-1}$ where J is in Jordan form.[2] We can write $J = D + N$ where D is the diagonal part of J and N is the rest, which is strictly upper triangular and hence nilpotent. Thus, $M = P(D+N)P^{-1} = PDP^{-1} + PNP^{-1}$, which is a decomposition into two matrices with the first diagonalizable and the second nilpotent.

We now show that D and N commute, which immediately implies that PDP^{-1} and PNP^{-1} also commute. The left action of D on N consists of scaling each row N_{i*} by the corresponding diagonal element D_{ii}, whereas the right action of D on N consists of scaling each column N_{*j} by D_{jj}. Now, $D+N$ is in Jordan normal form, so each row/column of N consists of at most a single 1 adjacent to and above the diagonal, and is otherwise uniformly 0. That means that such a 1 in row i and column $i+1$ will be scaled by D_{ii} under left-multiplication but by $D_{(i+1)(i+1)}$ under right-multiplication. But $N_{i(i+1)} = 1$ precisely if $D_{ii} = D_{(i+1)(i+1)}$! Thus, any nonzero entry in N will be scaled by the same factor under both left- and right-multiplication with D, so D and N commute. □

For an arbitrary matrix M, let $M = S + N$, with S diagonalizable, N nilpotent, and S and N commuting. We can thus compute $e^M = e^{S+N} = e^S e^N$ both of which we already know how to compute.

Example. Let

$$M = \begin{pmatrix} 3 & 1 & 0 & 1 \\ -1 & 5 & 4 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Then we seek to compute $\exp(M)$. By finding the roots of the characteristic polynomial, we find that the eigenvalues are 4, with algebraic multiplicity 3, and 2, with algebraic multiplicity 1. The eigenvectors corresponding to $\lambda = 4$ are $\langle 1,0,0,1\rangle^T$ and $\langle 1,1,0,0\rangle^T$, so $\lambda = 4$ has geometric multiplicity 2, and the eigenvector for $\lambda = 2$ is $\langle 1,-1,1,0\rangle^T$. We lack one dimension in the space of eigenvectors, so we seek an additional generalized eigenvector for $\lambda = 4$. We do this by squaring $(M-4I)$ and finding all solutions to $(M-4I)^2 v = 0$ that are not already solutions to $(M-4I)v = 0$. In this way, we find the generalized eigenvector $\langle -1,0,0,0\rangle^T$, with $(M-4I)\langle -1,0,0,0\rangle^T = \langle 1,1,0,0\rangle^T$. Thus, the Jordan normal form of M is:

$$\begin{aligned}
\begin{pmatrix} 3 & 1 & 0 & 1 \\ -1 & 5 & 4 & 1 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} = XJX^{-1} &= \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}^{-1} \\
&= X(S+N)X^{-1} = X \left[\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right] X^{-1}.
\end{aligned}$$

[2]For an accessible introduction to Jordan Normal form, see [4][5][6]

We have that S is a diagonal matrix, N is a nilpotent matrix (in particular, $N^2 = \mathbf{0}$), and S and N commute. This allows us to calculate:

$$\begin{aligned}
\exp(M) &= X\exp(S+N)X^{-1} = X\exp(S)\exp(N)X^{-1} \\
&= \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} e^4 & 0 & 0 & 0 \\ 0 & e^4 & 0 & 0 \\ 0 & 0 & e^4 & 0 \\ 0 & 0 & 0 & e^2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 0 & e^4 & e^2+e^4 & e^4 \\ -e^4 & 2e^4 & 3e^4-e^2 & e^4 \\ 0 & 0 & e^2 & 0 \\ 0 & 0 & 0 & e^4 \end{pmatrix}.
\end{aligned}$$

Remark 3.12. There is another way of calculating the matrix exponential of a non-diagonalizable matrix: Since there exists a sequence of diagonalizable matrices $D_1, D_2, \dots$ that converges to the matrix in question, we can calculate $\lim_{k\to\infty}\exp(D_k)$. For example, let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } D_k = \begin{pmatrix} 1 & 1 \\ \varepsilon^2 & 1 \end{pmatrix},$$

with $\varepsilon^2 = \frac{1}{k}$. It is straightforward to calculate that the eigenvalues of D_k are $1+\varepsilon, 1-\varepsilon$ with corresponding eigenvectors $\binom{1}{\varepsilon}, \binom{1}{-\varepsilon}$. Then we calculate:

$$\exp(D_k) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ \varepsilon & -\varepsilon \end{pmatrix}\begin{pmatrix} e^{1+\varepsilon} & 0 \\ 0 & e^{1-\varepsilon} \end{pmatrix}\begin{pmatrix} 1 & \frac{1}{\varepsilon} \\ 1 & -\frac{1}{\varepsilon} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} e^{1+\varepsilon}+e^{1-\varepsilon} & \frac{e^{1+\varepsilon}-e^{1-\varepsilon}}{\varepsilon} \\ \varepsilon e^{1+\varepsilon}-\varepsilon e^{1-\varepsilon} & e^{1+\varepsilon}+e^{1-\varepsilon} \end{pmatrix},$$

which converges to $\begin{pmatrix} e & e \\ 0 & e \end{pmatrix}$ as $\varepsilon \to 0$.

Proposition 3.13. *If M is a complex square matrix,* $\det(e^M) = e^{tr(M)}$

Proof. Consider an arbitrary diagonalizable matrix $M = PDP^{-1}$ with eigenvalues $\lambda_1, \lambda_2, \cdots \lambda_n$. Then

$$e^{\mathrm{tr}(M)} = e^{\sum_{i=1}^n \lambda_i}$$

and

$$\det(e^M) = \det(Pe^DP^{-1}) = \det(P)\det(e^D)\det(P^{-1}) = \det(e^D) = \prod_{i=1}^n e^{\lambda_i}.$$

These two are clearly equal, as desired.

Any matrix M can be approximated arbitrarily well by a sequence of diagonalizable matrices, A_n (by Lemma 3.8), each of which satisfies $\det(e^{A_n}) = e^{\mathrm{tr}(A_n)}$. Each of these functions are continuous and the composition of continuous functions is continuous, so taking limits, we have $\det(e^M) = e^{\mathrm{tr}(A_n)}$ for any M as desired.

□

Corollary 3.14. *If M is a complex square matrix, e^M is an invertible matrix.*

Proof. Because $\det(e^M) = e^{\mathrm{tr}(M)} \neq 0$, e^M is invertible.

Alternatively, because A and $-A$ commute, $e^Ae^{-A} = e^{\mathbf{0}} = I$, so e^{-A} is the inverse of e^A □

Definition 3.15. The matrix logarithm of a square matrix M is defined as the power series

$$\log(M) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(M-I)^n$$

wherever this series converges.

Proposition 3.16. *The matrix logarithm is defined and continuous for square matrices M with $||M-I|| < 1$.*

We proceed by a similar argument to the matrix exponential. We have

$$\sum_{n=1}^{\infty} \left\| \frac{(-1)^{n-1}}{n}(M-I)^n \right\| \leq \sum_{n=1}^{\infty} \frac{1}{n}||M-I||^n$$

which converges when $||M-I|| < 1$. Thus the matrix logarithm absolutely converges, and hence converges for $||M-I|| < 1$.

This series converges uniformly by the Weierstrass M-test and has continuous partial sums, so the logarithm is continuous on $||M-I|| < 1$.

Proposition 3.17. *The matrix logarithm is the inverse of the matrix exponent. Namely, if $\|M-I\| < 1$, $e^{\log(M)} = Mf$, and if $\|M\| < \log 2$, $\log e^M = M$.*

Proof. First, suppose that the matrix M is diagonalizable. Write $M = V\Lambda V^{-1}$, so $M - I = V\Lambda V^{-1} - I = V(\Lambda - I)V^{-1}$. Note that none of the eigenvalues may be zero, since otherwise we would have $\|M-I\| \geq 1$. It then follows that $(M-I)^n$ is of the form

$$(M-I)^n = V \begin{pmatrix} (\lambda_1 - 1)^n & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & (\lambda_m - 1)^n \end{pmatrix} V^{-1}.$$

If $\|M-I\| < 1$, then $|\lambda_i - 1| < 1$ for all i. In this case, therefore, we have

$$\begin{aligned} \log(M) &= V \sum_{n=1}^{\infty} \begin{pmatrix} (-1)^{n-1}\frac{(\lambda_1-1)^n}{n} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & (-1)^{n-1}\frac{(\lambda_m-1)^n}{n} \end{pmatrix} V^{-1} \\ &= V \begin{pmatrix} \log(\lambda_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \log(\lambda_m) \end{pmatrix} V^{-1}. \end{aligned}$$

Thus,

$$\exp(\log(M)) = V \begin{pmatrix} \exp(\log(\lambda_1)) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \exp(\log(\lambda_m)) \end{pmatrix} V^{-1} = V \begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_m \end{pmatrix} V^{-1} = M.$$

Conversely, if $\|M\| < \log(2)$, then

$$\|\exp(M) - I\| = \|\sum_{n=1}^{\infty} \frac{M^n}{n!}\| \leq \sum_{n=1}^{\infty} \frac{\|M\|^n}{n!} = \exp(\|M\|) - 1 < 1,$$

so $\log(\exp(M))$ converges. Decomposing M again into $V\Lambda V^{-1}$ and making similar computations as when computing $\exp(\log(M))$, we find that it converges to M.

If M is not diagonalizable, then because the diagonalizable matrices are dense within the space of all matrices, there must exist a sequence of diagonalizable matrices $D_1, D_2, D_3, \dots$ that converges to M. Since $\exp(\log(D_i)) = \log(\exp(D_i)) = D_i$ and the log and exp functions are continuous, we must have $\exp(\log(M)) = \log(\exp(M)) = M$. □

Remark 3.18. This result also holds without the magnitude requirements for all nilpotent matrices $M - I$. First, the logarithm sum will be finite, so it will converge. Next, we can check that the logarithm is still the inverse of the exponential with the same argument, that is, proving that this is the case for a converging sequence of diagonalizable matrices. This is valid to do because the eigenvalues of M will all be equal to 1 (since the eigenvalues of a nilpotent matrix $M - I$ must all be zero), so that the sum $\sum_{n=1}^{\infty}(-1)^{n-1}\frac{(\lambda_i - 1)^n}{n}$ will converge to $\log(\lambda_i)$ for λ_i sufficiently close to 1. Furthermore, $\log(\exp(M)) = M$ will still hold, as the exponential of a nilpotent matrix remains nilpotent.

Remark 3.19. We can extend the definition of the logarithm to all invertible matrices M in the following manner. First, suppose M is diagonalizable, so that $M = V\Lambda V^{-1}$, with eigenvalues $\lambda_1, \lambda_2, \dots, \lambda_m$. Then we define the matrix logarithm as

$$V \begin{pmatrix} \log(\lambda_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \log(\lambda_m) \end{pmatrix} V^{-1},$$

for a suitable branch cut for each of the logarithms (preferably a consistent one). If M is not diagonalizable, then we can just use in its place a converging sequence of diagonalizable matrices. Note that although we will certainly have $\exp(\log(M)) = M$ for all invertible M, we will not have in general have $\log(\exp(M)) = M$ at or beyond a distance of 1 from the identity due to the multi-valued nature of the complex logarithm.

We can practically calculate the logarithm of a nondiagonalizable matrix M in a similar way to the case of the exponential. First, as just mentioned, we can approximate it arbitrarily well with a diagonalizable matrix. Second, we can also decompose M into its Jordan normal form $M = XJX^{-1}$. Now, J can be expressed as $S(N + I)$, where S is a diagonal matrix containing the diagonal elements of J, and N is a strictly upper triangular and thus nilpotent matrix. Now, $\log(S)$ is still a diagonal matrix, and $\log(N + I) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{N^n}{n}$, where the n^{th} matrix in the sum has nonzero entries only at indices $(i, i + n)$, with i such that $S_{ii} = S_{(i+n)(i+n)}$. Therefore, since left-multiplying $\log(N + I)$ by $\log(S)$ scales $\log(N + I)_{i(i+n)}$ by $\log(S)_{ii}$ and right-multiplying scales it by $\log(S)_{(i+n)(i+n)}$, $\log(S)$ and $\log(N+I)$ commute, so by Proposition 3.4, we have

$$\log(XS(N + I)X^{-1}) = X\log(S(N + I))X^{-1} = X(\log(S) + \log(N + I))X^{-1}.$$

Now, we know how to calculate $\log(S)$ because S is diagonal, and since N is nilpotent, $\log(N + I) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{N^n}{n}$ is a finite sum that is easy to calculate. This allows us to calculate the logarithm $\log(M)$.

Having the logarithm at our disposal allows us to prove the following proposition.

Proposition 3.20. *If A and B are complex square matrices, then* $e^{A+B} = \lim_{n\to\infty}(e^{A/n}e^{B/n})^n$

Proof. Multiplying the power series of $e^{A/n}$ and $e^{B/n}$, we see that

$$e^{A/n}e^{B/n} = I + \frac{A}{n} + \frac{B}{n} + O\left(\frac{1}{n^2}\right).$$

Now, $e^{A/n}e^{B/n}$ tends to I as $n \to \infty$, so its logarithm as a power series is well-defined and converges, so we calculate:

$$\begin{aligned}\log(e^{A/n}e^{B/n}) &= \log\left(I + \frac{A}{n} + \frac{B}{n} + O\left(\frac{1}{n^2}\right)\right)\\ &= \frac{A}{n} + \frac{B}{n} + O\left(\left\|\frac{A}{n} + \frac{B}{n} + O\left(\frac{1}{n^2}\right)\right\|^2\right)\\ &= \frac{A}{n} + \frac{B}{n} + O\left(\frac{1}{n^2}\right).\end{aligned}$$

Taking the exponential of both sides gives us

$$\begin{aligned} e^{A/n}e^{B/n} &= \exp\left(\frac{A}{n} + \frac{B}{n} + O\left(\frac{1}{n^2}\right)\right)\\ \implies (e^{A/n}e^{B/n})^n &= \exp\left(A + B + O\left(\frac{1}{n}\right)\right).\end{aligned}$$

Thus, by the continuity of the exponential, we have

$$\lim_{n\to\infty}(e^{A/n}e^{B/n})^n = \lim_{n\to\infty}\exp\left(A + B + O\left(\frac{1}{n}\right)\right) = \exp(A+B).$$

□

Lemma 3.21. *There exists a constant c such that for all $B \in \mathrm{M}_n(\mathbb{K})$ with $\|B\| < \frac{1}{2}$,*

$$\|\log(I+B) - B\| \le c\|B\|^2.$$

Proof. We calculate:

$$\begin{aligned}\log(I+B) - B = \sum_{n=2}^{\infty}(-1)^{n-1}\frac{B^n}{n} &= B^2\sum_{m=2}^{\infty}(-1)^{n-1}\frac{B^{n-2}}{m}\\ \implies \|\log(I+B) - B\| &\le \|B\|^2\sum_{n=2}^{\infty}\frac{\left(\frac{1}{2}\right)^{n-2}}{n}.\end{aligned}$$

The lemma is proven by letting $c = \sum_{n=2}^{\infty}\frac{\left(\frac{1}{2}\right)^{n-2}}{n}$. □

We now use this lemma to prove a very nice interpretation of the matrix exponential, which is a generalization of the identity $\lim_{n\to\infty}(1+\frac{x}{n})^n = e^x$, with $x \in \mathbb{C}$.

Proposition 3.22. *Let $A \in \mathrm{M}_n(\mathbb{K})$ and $C_n \in \mathrm{M}_n(\mathbb{K})$ with $C_n = O\left(\frac{1}{n^2}\right)$. Then*

$$\lim_{n\to\infty}\left(I + \frac{A}{n} + C_n\right)^n = \exp(A).$$

Proof. The parenthesized expression tends towards I as $n \to \infty$, so it is within the domain of the logarithm for sufficiently large n. We can thus apply the logarithm to it, obtaining

$$\log\left(I + \frac{A}{n} + C_n\right) = \frac{A}{n} + C_n + E_n,$$

where E_n is an error term satisfying, by the preceding lemma, $E_n = O\left(\left\|\frac{A}{n} + C_n\right\|^2\right) = O\left(\frac{1}{n^2}\right)$. We then have

$$I + \frac{A}{n} + C_n = \exp\left(\frac{A}{n} + C_n + E_n\right)$$
$$\implies \left(I + \frac{A}{n} + C_n\right)^n = \exp(A + nC_n + nE_n) = \exp\left(A + O\left(\frac{1}{n}\right)\right),$$

which converges to $\exp(A)$ as $n \to \infty$. □

Definition 3.23. The commutator bracket is defined as $[A, B] = AB - BA$.

We know that if two matrices A and B commute, then $\log(\exp(A)\exp(B)) = A + B$. The following is a generalization of this result.

Theorem 3.24 (Baker-Campbell-Hausdorff formula)**.** *We have*

$$\log\big(\exp(A)\exp(B)\big) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \sum_{\substack{r_1+s_1>0 \\ \vdots \\ r_n+s_n>0}} \frac{[A^{(r_1)}B^{(s_1)}A^{(r_2)}B^{(s_2)} \dots A^{(r_n)}B^{(s_n)}]}{\sum_{j=1}^{n}(r_j + s_j)\Pi_{i=1}^{n} r_i! s_i!},$$

where the notation $M^{(k)}$ denotes composition of M with itself k times under the commutator operation—that is $[M^{(k)}A] = [M, [M^{(k-1)}A]]$ with $[M^{(1)}A] = [M, A]$—and the notation $[M_1 M_2 \dots M_k]$ denotes $[M_1, [M_2, \dots, [M_k] \dots]]$. This expression converges for sufficiently small A and B. The first few terms of this sum are given by

$$\log\big(\exp(A)\exp(B)\big) = A + B + \frac{1}{2}[A, B] + \frac{1}{12}[A, [A, B]] + \frac{1}{12}[B, [B, A]] \dots$$

If A and B are sufficiently small, we sometimes make the approximation $\exp(A)\exp(B) \approx \exp(A + B)$*.*

We omit the proof, although the interested reader can find multiple proofs at [16]. Note in particular that $\log(\exp(A)\exp(B))$ is completely determined by the commutators of A and B, which is not obvious from simply expanding the power series. This will have important implications when we study the Lie group-Lie algebra correspondence in the next section.

4. Lie Algebras

Definition 4.1. A Lie algebra over $\mathbb{K}$ is a vector space $\mathfrak{g}$ with a Lie bracket $[,] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ where for all $x, y, z \in \mathfrak{g}$ and $a, b \in \mathbb{K}$:

- $[ax + by, z] = a[x, z] + b[y, z]$ and $[x, ay + bz] = a[x, y] + b[x, z]$ (billinear),
- $[x, y] = -[y, x]$ (skew symmetric),
- and $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi identity).

Example. The vector space $\mathfrak{g} = \mathbb{R}^3$ under the cross product ($[x, y] = x \times y$) is a Lie Algebra.

Definition 4.2. Let $f(t) : \mathbb{R} \to M_n(\mathbb{K})$ be a matrix-valued function. Then the derivative at x is

$$f'(x) = \lim_{t \to 0} \frac{f(x + t) - f(x)}{t}.$$

Remark 4.3. This derivative behaves exactly as we would expect, following the product and chain rule.

Definition 4.4. The tangent space to a matrix group G at g is the set of all tangent vectors at g for all paths γ that go through g.

$$T_g(G) = \{\gamma'(0) | \gamma : (-\varepsilon, \varepsilon) \to G \text{ differentiable with } \varepsilon > 0 \text{ and } \gamma(0) = g\}$$

Proposition 4.5. *The tangent space is a real vector subspace of* $M_n(\mathbb{K})$

Proof. Let a, b be in the tangent space at g, with γ_1 and γ_2 be curves with $\gamma_1'(0) = a$ and $\gamma_2'(0) = b$. Let c be a real scalar.

We show $a + b$ is also in the tangent space. Consider $\gamma(t) = \gamma_1(t)g^{-1}\gamma_2(t)$ which is defined on some open interval around 0. By the product rule, we have

$$\gamma'(0) = \gamma_1'(0)g^{-1}\gamma_2(0) + \gamma_1(0)g^{-1}\gamma_2'(0) = ag^{-1}g + gg^{-1}b = a + b$$

so the tangent space is closed under addition.

We now show ca is in the tangent space. Consider $\gamma(t) = \gamma_1(ct)$ which is defined on some open interval around 0. By the chain rule, $\gamma'(0) = c\gamma_1'(0) = ca$ as desired. □

Theorem 4.6. *A matrix M is in the tangent space of G if and only if $e^{tM} \in G$ for all $t \in \mathbb{R}$.*

Proof. If $\gamma(t) = e^{tM} \in G$ for all $t \in \mathbb{R}$, then $\gamma'(0) = Me^{0M} = M$ is the tangent space of G at its identity. This completes the reverse direction.

We now show the converse. If M is in the tangent space of G at its identity, then there must exist a curve $\gamma : (-\varepsilon, \varepsilon) \to G$ with $\gamma(x) = I + Mx + O(x^2)$ as $x \to 0$. Replacing x with $\frac{t}{n}$ for any $t \in \mathbb{R}$, we have $\gamma(\frac{t}{n}) = I + \frac{Mt}{n} + O\left(\frac{1}{n^2}\right)$ as $n \to \infty$. Since $\gamma(\frac{t}{n}) \in G$, we surely have $\gamma(\frac{t}{n})^n$ for any n. Taking the limit as $n \to \infty$ yields

$$\begin{aligned}
\lim_{n\to\infty} \gamma\left(\frac{t}{n}\right)^n &= \lim_{n\to\infty} \left(I + \frac{Mt}{n} + O\left(\frac{1}{n^2}\right)\right)^n \\
&= e^{tM} && \text{(by Proposition 3.22)} \\
&\in G.
\end{aligned}$$

□

Proposition 4.7. *Let G be a matrix group with Lie algebra $\mathfrak{g}$. If X and Y are elements of $\mathfrak{g}$, then the following hold:*

(1) *$AXA^{-1} \in \mathfrak{g}$ for all $A \in G$,*
(2) *$XY - YX \in \mathfrak{g}$.*

Proof. For the first point, we see that for all $t \in \mathbb{R}$,

$$\exp(t(AXA^{-1})) = \exp(A(tX)A^{-1}) = A\exp(tX)A^{-1} \in G.$$

We now prove the second point. We use the product rule and Proposition 3.5 to compute

$$\begin{aligned}
\frac{d}{dt}\left(e^{tX}Ye^{-tX}\right)\Big|_{t=0} &= (XY)e^0 + (e^0Y)(-X) \\
&= XY - YX.
\end{aligned}$$

By the first point, $e^{tX}Ye^{-tX} \in \mathfrak{g}$ for all t. Since we have already shown that $\mathfrak{g}$ is a vector space, it follows that

$$XY - YX = \lim_{h\to 0} \frac{e^{hX}Ye^{-hX} - Y}{h} \in \mathfrak{g}.$$

□

Proposition 4.8. *The commutator bracket satisfies the properties of a Lie bracket.*

Proof. We can straightforwardly check each of the properties. Let c_1, c_2 be arbitrary scalars and let A, B, C be arbitrary matrices. Then

$$\begin{aligned}[c_1A + c_2B, C] &= (c_1A + c_2B)C - C(c_1A + c_2B) \\ &= c_1(AC - CA) + c_2(BC - CB) \\ &= c_1[A, C] + c_2[B, C],\end{aligned}$$

with $[C, c_1A + c_2B]$ following similarly. It is also clear

$$[A, B] = AB - BA = -(BA - AB) = -[B, A].$$

The last condition can be checked by fully expanding

$$\begin{aligned}[A, [B, C]] + [B, [C, A]] + [C, [A, B]] &= [A, BC - CB] + [B, CA - AC] + [C, AB - BA] \\ &= ABC - ACB - BCA + CBA + BCA - BAC \\ &\quad - CAB + ACB + CAB - CBA - ABC + BAC \\ &= 0,\end{aligned}$$

as every term cancels once. □

Definition 4.9. The Lie Algebra $\mathfrak{g}$ of a matrix group G is the tangent space at the identity with the Lie bracket as the commutator bracket.

Remark 4.10. We have checked that $\mathfrak{g}$ is a vector space (Prop 4.5), the commutator bracket is well defined (Prop 4.7), and that the commutator bracket is a Lie Bracket (Prop 4.8), justifying our definition.

Remark 4.11. We have checked that the tangent space is a vector space and that the commutator satisfies the definition of a Lie bracket, but this definition is still not yet fully justified as we must check the Lie Bracket is closed in $\mathfrak{g}$. We will verify this later.

Example. The Lie Algebra of $\mathrm{GL}_n(\mathbb{C})$ is $M_n(\mathbb{C})$.

Proof. For any matrix M and real t, e^{tM} is invertible, and thus must be in $\mathrm{GL}_n(\mathbb{C})$. □

Example. The Lie Algebra of $\mathrm{GL}_n(\mathbb{R})$ is $M_n(\mathbb{R})$.

Proof. If M is a real matrix and t is real, e^{tM} is an invertible real matrix, and thus must be in $\mathrm{GL}_n(\mathbb{R})$.

For the converse, note that if e^{tM} is a real invertible matrix for all real t, $M = \frac{d}{dt}e^{tM}|_{t=0}$ must be real. □

Example. The Lie Algebra of $SL_n(\mathbb{C})$ are the n by n complex matrices with trace 0. The Lie Algebra of $SL_n(\mathbb{R})$ are the n by n real matrices with trace 0.

Proof. If M has trace 0 and t is real, we have $\det e^{tM} = e^{\mathrm{tr}(tM)} = e^0 = 1$, so $e^{tM} \in SL_n(\mathbb{C}$ for all real t.

For the converse, if e^{tM} has determinant 1 for all real t,

$$\mathrm{tr}(M) = \frac{d}{dt}e^{t\mathrm{tr}(M)})|_{t=0} = \frac{d}{dt}\det(e^{tM})|_{t=0} = \frac{d}{dt}1|_{t=0} = 0$$

as desired.

The Lie Algebra of $SL_n(\mathbb{R})$ follows similarly. □

Example. The Lie algebra of $U(n)$ is the vector space of n by n complex matrices M with $M^* = -M$ (skew Hermitian matrices). The Lie Algebra of $SU(n)$ is the vector space of n by n skew Hermitian complex matrices with trace 0. The Lie Algebra of $O(n)$ is the vector space of all real skew-symmetric matrices ($M^T = -M$). The Lie Algebra of $SO(n)$ is the vector space of all real skew-symmetric matrices with trace 0.

Proof. A matrix U is unitary if and only if $U^* = U^{-1}$, so e^{tX} is unitary if and only if

$$e^{tX^*} = (e^{tX})^* = (e^{tX})^{-1} = e^{-tX},$$

which in turn is true for all real t if and only if $X^* = -X$.

The Lie Algebras for $SU(n), O(n)$, and $SO(n)$ all follow similarly. □

Definition 4.12. If $\mathfrak{g}, \mathfrak{h}$ are $\mathbb{K}$ Lie Algebras, a $\mathbb{K}$-linear transformation $\Phi : \mathfrak{g} \to \mathfrak{h}$ is a homomorphism of Lie algebras if for all $x, y \in \mathfrak{g}$,

$$\Phi([x, y]) = [\Phi(x), \Phi(y)].$$

Definition 4.13. Suppose that $G \leqslant GL_n(\mathbb{K})$ and $H \leqslant GL_m(\mathbb{K})$ are matrix groups with a continous map $\varphi : G \to H$. φ is a differentiable map if:

(1) For every smooth curve $\gamma : (a, b) \to G$, $\varphi \circ \gamma : (a, b) \to H$ is also differentiable.
(2) If there exist two differentiable curves $\gamma, \tilde{\gamma} : (a, b) \to G$ such that $\gamma(0) = \tilde{\gamma(0)}$ and $\gamma'(0) = \tilde{\gamma'(0)}$ then
$$(\varphi \circ \gamma)'(0) = (\varphi \circ \tilde{\gamma})'(0).$$

A continuous homomorphism of matrix groups is a Lie homomorphism if it also a differentiable map. To give some intuition for this definition, we should expect a derivative to be a function between tangent spaces. We write $d\varphi$ to be a homomorphism from a Lie algebra to a Lie algebra as Lie algebras are the tangent spaces to a Lie group at the identity.

Theorem 4.14. *Suppose that G and H are matrix groups with a differentiable homomorphism $\varphi : G \to H$. Then, the derivative $d\varphi : \mathfrak{g} \to \mathfrak{s}$ is a Lie homomorphism.*

We omit the proof for brevity.

5. Representation of Lie Groups

Definition 5.1. A representation (ρ, V) of a group G over some vector space V is the group homomorphism defined by $\rho : G \to GL(V)$.

In this definition, $GL(V)$ denotes the group of invertible linear maps from V to itself. To see that this is the same as our previous definition of $GL(V)$, recall from linear algebra that a linear map can be written as a matrix where the column vectors are the map applied to the elements of a basis of V. Thus, it must be true that there exists an isomorphism such that $GL(V) \simeq GL_n(F)$ where $n = \dim(V)$ and is called the dimension of the representation ρ. Note that this is only true when n is finite.

Let's now discuss some types of representations. One kind of representation is a representation that preserves the Hermitian inner product on a space.

Definition 5.2. A representation (ρ, V) where V is a complex vector space, is unitary if,

$$\langle \rho(g)v_1, \rho(g)v_2 \rangle = \langle v_1, v_2 \rangle$$

for all $g \in G$, and $v_1, v_2 \in V$, where $\langle ., . \rangle$ is the Hermitian inner product on V

Now, let us consider representations where the group is a Lie group, G. Then, we only consider the ρ which along with being a valid representation, are also differentiable maps. Thus, for a representation (ρ, V) with the domain being a Lie group, the codomain in this case, $GL_n(\mathbb{C})$, is isomorphic to $\mathbb{C}^{n^2}$, without the non-invertible matrices. We will now classify some common representations into certain categories.

Definition 5.3. An irreducable representation is a representation ρ, for which there there are no nonzero subspaces $S \subset V$, such that (ρ, S) is a representation.

Definition 5.4. An reducable representation is a representation ρ, for which there there are nonzero subspace(s) $S \subset V$, such that (ρ, S) is a representation.

Consider combining two representations.

Definition 5.5. Suppose that ρ_1 and ρ_2 are the representations of dimensions n_1 and n_2 respectively. Then, there exists a representation with dimension $n_1 + n_2$, the direct sum of the two aforementioned representations, denoted by $\rho_1 \oplus \rho_2$. The direct sum is defined by

$$(\rho_1 \oplus \rho_2) : g \in G \to \begin{bmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{bmatrix}$$

Proposition 5.6. *Every unitary representation can be expressed as the direct sum of irreducible representations.*

Proof. Suppose that ρ is an reducible representation of G on V. Then, by the definition of an reducible representation, there is some subspace $W \subset V$ such that $(\rho_{|W}, W)$, where $\rho_{|W}$ is the representation limited to group elements corresponding with elements of W, and the equation

$$(\rho, V) = (\rho_{|W}, W) \oplus (\rho_{|W^\perp}, W^\perp)$$

is satisfied. Recall that unitary representations preserve the Hermitian inner product. This then implies that $(\rho_{|W^\perp}, W^\perp)$ is a subrepresentation. To decompose ρ into the desired direct sum of irreducible representations, we can continue applying this method to W and $W^\perp$. □

A classical result of representation theory is Schur's lemma. In this text, we will present and prove only the second part as that is the part of the lemma which will be utilized in the further section on quantum theory.

Lemma 5.7 (Schur's Lemma)**.** *Let V be a vector space and $\rho : G \to GL_n(\mathbb{C})$ be an irreducible representation. All linear maps $L : V \to V$ for which $L(\rho(g)(v)) = \rho(g)(L(v))$ where v and g are elements of V and G respectively, are scalar multiples of* $\mathbf{1}$.

Proof. The eigenvalues λ of L are the solutions to $\det(L - \lambda\mathbf{1}) = 0$. Thus the eigenspaces of L can be written as $\ker(L - \lambda\mathbf{1})$. Because L commutes for all $\rho(g), \rho(g)(v) \in \ker(L - \lambda\mathbf{1})$ if v is an element of the kernel of $L - \lambda\mathbf{1}$. This implies that $(\rho_{|\ker(L-\lambda\mathbf{1})}, \ker(L - \lambda\mathbf{1}))$ is a representation of G. If V is irreducible, we must have that $\ker(L - \lambda\mathbf{1})$ is either 0 or V and is V because λ is an eigenvalue, implying the result. □

Remark 5.8. The lemma is only true for complex vector spaces V as the eigenvalues λ of L are not the solutions of $\det(L - \lambda\mathbf{1}) = 0$ for a real vector space.

The following result directly follows from the definition of an abelian group and Schur's lemma.

Corollary 5.9. *All irredudible representations of an abelian group have dimension* 1.

Consider the points on the complex unit circle. This is the group of all complex numbers with absolute value one. Each point can also be written as $e^{i\theta}$ for angle of rotation θ. This group of points is denoted as $\mathbb{S}^1$ and is sometimes called the circle group. Now, note that each point $e^{i\theta}$ can be expressed as a 1 by 1 matrix,

$$P = \begin{bmatrix} e^{i\theta} \end{bmatrix}.$$

It is also true that

$$P^*P = \begin{bmatrix} e^{i\theta} \end{bmatrix} \begin{bmatrix} e^{-i\theta} \end{bmatrix} = I.$$

Furthermore if $M = [z]$ has the property $M^*M = I$, then $\bar{z}z = 1$, so $|z| = 1$. Thus, any matrix in $U(1)$ must be of the form $[e^{i\theta}]$ for some θ. Henceforth the group of complex numbers with absolute value 1 is the unitary group $U(1)$. Since $U(1)$ is abelian, Corollary 5.9 implies that all irreducible representations of it has dimension one.

Proposition 5.10. *Each representation of $U(1)$ is unitary and can be written as*

$$\rho_k : e^{i\theta} \in U(1) \to e^{i\theta k} \in GL_1(\mathbb{C})$$

where $k \in \mathbb{Z}$.

Proof. Let each representation ρ_k be in terms of a rotation angle $\theta \in \mathbb{R}$. We then have the following properties of ρ_k :

(1) $\rho_k(0) = 1 = \rho_k(2\pi)$
(2) $\rho_k(\theta_1 + \theta_2) = \rho_k(\theta_1)\rho_k(\theta_2)$

Now consider representations which are differentiable maps of the form $f : U(1) \to GL_1(\mathbb{C})$ that are also in terms of θ and thus also have the aforementioned properties. By the definition of the derivative,

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

Because $f(0) = 1, f(\theta) = e^{f'(0)\theta}$ and condition one implies that $f = \rho_k$, one of the representations of $U(1)$. ☐

6. Quantum Theory

There are many applications of Lie groups and Lie algebras to the field of quantum theory. This is due to Lie groups being able to model the symmetric phenomena in quantum theory. We begin with the Dirac-von Neumann axioms. A system in quantum theory is essentially a collection of relevant structures. A system includes states, observables, and a law for its dynamics. One interpretation of the state of a quantum system is a vector in the space of solutions to some equation for motion [14].

Axiom 6.1. The state of a system is a non-zero vector, $\mathbf{v}$ in a complex vector space $\mathcal{H}$ in which there is a Hermitian inner product $\langle \cdot\ ,\ \cdot \rangle$.

Observables are quantities in a system that can be "observed". One important observable in a quantum state is the Hamiltonian, H, which is used for finding how states can change over time. The Hamiltonian is an operator that provides the total energy of the system at some time t.

Axiom 6.2. The observables of a system are given by self-adjoint linear operators on $\mathcal{H}$.

As per bra-ket notation, a state vector $\psi \in \mathcal{H}$ is written as $|\psi\rangle$.

Axiom 6.3. Let $|\psi(t)\rangle \in \mathcal{H}$ be the state of the system at time t. Then, the time evolution of states is given by the operator H, where

$$H\|\psi(t)\rangle = \frac{d}{dt}|\psi(t)\rangle\hbar i$$

in which $\hbar$ is Planck's constant and i is the imaginary number $\sqrt{-1}$

Planck's constant, h, is theoretically equal to the energy of a photon divided by its frequency. Experimentally, h is approximately equal to $6.626\frac{J}{Hz}$, J and Hz denoting joules (energy) and hertz (frequency) respectively. The reduced Planck constant, $\hbar$, can be expressed as

$$\hbar = \frac{h}{2\pi} = 1.055 \times 10^{-32} J \cdot s.$$

As per [14], $\hbar$ depends on the units it is expressed in, so units can be chosen such that $\hbar = 1$, which can simply many computations. The Dirac-von Neumann axioms of quantum theory have some limitations, including their limited viability to larger-scale systems. Suppose that some group G is acting on a quantum system. Then, the state space $\mathcal{H}$ must have a unitary representation of G. This fact is useful, as it is mentioned in [14] that each physical system with a group acting on it has a representation of the group. Recall from the definition of a representation that $\rho(g) \in GL_n(\mathbb{C})$.

If we have $g \in G$ which is "close" to the identity $e \in G$, and some $\rho(g) \in GL_n(\mathbb{C})$, then it is true that $\rho(g) = e^A$ for some matrix A that is "close" to the zero matrix. It can also be shown that the conjugate transpose of A is $-A$, and the conjugate transpose of iA is iA. Thus, it is clear that some representation ρ from G on $\mathcal{H}$ gives corresponding self-adjoint operators on $\mathcal{H}$.

Example. Let's see an example of this phenomenon from [14]. Let our group G be translations in time. Using the aforementioned facts, there is a unitary representation of G on $\mathcal{H}$ defined by

$$t \in G \to \rho(t) \in GL(\mathcal{H}) = e^{-\frac{Hit}{\hbar}}.$$

Consider the representation of $U(1)$ on the state space $\mathcal{H}$. If ρ is irreducible, it must be one-dimensional and have the form $(\rho_k, \mathbb{C})$. It is also true that $\mathcal{H} = \mathcal{H}_{k_1} \oplus \mathcal{H}_{k_2} \oplus \cdots \oplus \mathcal{H}_{k_n}$ where $n = \dim(\mathcal{H})$ and the $\mathcal{H}_{k_j}$ are isomorphic to $\mathbb{C}$ and correspond to the representation ρ_{k_j}. Recall that because $\mathcal{H}$ is the representation of a Lie group, there exists an associated linear operator on $\mathcal{H}$. This is denoted as Q and is named the charge operator.

Definition 6.4. The charge operator Q is the self adjoint linear operator which acts by multiplication of by k_j on the irreducible sub-representation $\mathcal{H}_{k_j}$. This is defined for the representation of $U(1)$ on $\mathcal{H}$ denoted by ρ.

We may also write Q as a matrix $A \in M_n(\mathbb{Z})$ where $A_{j,j} = k_j$ for all q_j. All other elements of A are 0. It is possible to obtain this operator from the group action of $U(1)$ on $\mathcal{H}$ defined by

$$\rho_1(e^{i\theta}) = e^{iQ\theta}.$$

Taking the matrix exponential gives the matrix

$$e^{iQ\theta} = \begin{pmatrix} e^{ik_1\theta} & 0 & \dots & \dots & 0 \\ 0 & e^{ik_2\theta} & \dots & 0 & \dots \\ \dots & 0 & & 0 & \dots \\ \dots & \dots & \dots & & 0 \\ 0 & 0 & \dots & 0 & e^{ik_n\theta} \end{pmatrix}$$

which is obviously an element of $U(n)$.

Theorem 6.5 (Noether)**.** *In a quantum system with a continuous symmetry property, there exist some quantities of whose values are conserved throughout time.*

The values of these quantities remain constant as the time t changes. One example of this theorem is the charge operator Q. Using the formal definition of a state, and other physical concepts which are out of the scope of the paper, one can mathematically show that

$$|\psi(t)\rangle = e^{-itH}|\psi(0)\rangle$$

when H is time-independent. It is common to let $U(t) = e^{-itH}$ and this is commonly called the time evolution operator.

Since we may express operators as matrices, we can use the previously defined commutator bracket on two operators. Suppose that the Hamiltonian H and the charge Q commute. This implies that e^{-itH} must also commute with Q so we get

$$[U(t), Q] = 0 \implies U(t)Q = QU(T).$$

Using this equation, now note that

$$Q|\psi(t)\rangle = QU(t)|\psi(0)\rangle = U(t)Q|\psi(0)\rangle = U(t)k_j|\psi(0)\rangle = q_j|\psi(t)\rangle$$

assuming that k_j is well-defined at time 0. This equation implies that k_j will not change throughout time. Because $U(t)$ and Q commute,

$$U(t)\rho_1(e^{i\theta}) = \rho_1(e^{i\theta})U(t).$$

Thus, the representation ρ_1 of $U(1)$ on $\mathcal{H}$ commutes with the time evolution law.

This example of the conservation of Q motivates the following concept.

Principle 6.6. If an observable O and the Hamiltonian observable H commute, one can obtain a conservation law from the relation.

7. Motion Detection

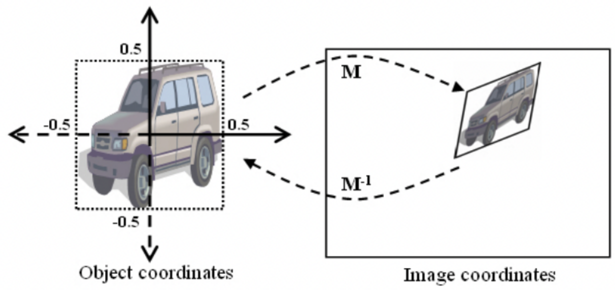
Tuzel et al [13] develop an interesting application of Lie groups to object tracking. We are given the pixel values of a reference image of some object, such as a car, that is constrained within the unit square about the origin. Suppose we are also given an image containing that car. Now, the pixel values of the car in the actual image won't correspond necessarily to those in the reference image, since the perception angle may be different. However, there is some affine transformation M that approximately maps the reference image to the affine region containing the car in the actual image. In particular, M is of the form

$$M = \begin{pmatrix} A & \mathbf{b} \\ \mathbf{0} & 1 \end{pmatrix},$$

for any matrix A, and the image coordinates $(x_{\text{img}}, y_{\text{img}})$ are related to the object coordinates $(x_{\text{obj}}, y_{\text{obj}})$ by

$$\begin{pmatrix} x_{\text{img}} \\ y_{\text{img}} \\ 1 \end{pmatrix} = M \begin{pmatrix} x_{\text{obj}} \\ y_{\text{obj}} \\ 1 \end{pmatrix}.$$

An illustration is shown below [13].

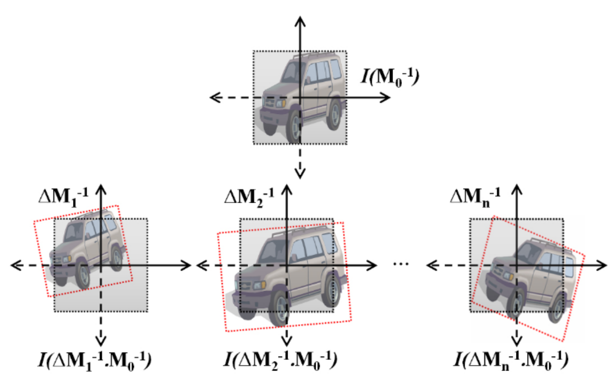


As the object moves, however, M will change. At each time-step t, therefore, we update the transformation matrix by right-multiplying by an estimated difference matrix: $M_t = M_{t-1}\Delta M_t$. We thus seek to estimate ΔM_t at each time step.

In order to lower the dimensionality of the reference image for our models, we convert its raw pixel values into a grid of orientation histograms. For example, after discarding the outer 10% of the reference image (because the borders of the reference image are usually contaminated by the background), we divide what remains into a 6×6 grid of tiles. For each tile, we compute the gradient of each pixel, whose direction is discretized to be one of the eight compass directions, and create a histogram of the gradient directions weighted by the gradient magnitudes. This lowers the dimensionality of the input to $36 \cdot 8 = 288$ dimensions. Given an affine transformation matrix M, we denote the corresponding unit-square reference image as $I(M^{-1})$ and its orientation histogram as $o(M^{-1})$. We thus seek to learn a regression function f such that at each time step, we have

$$\Delta M_t = f\big(o(M_{t-1}^{-1})\big).$$

At time 0, the reference image of the object and the initial transformation matrix M_0 are given. We generate an initial training dataset as follows. First, we generate n random affine transformation matrices $\{\Delta M_1^i : i \in [1, n]\}$ around the identity matrix (according to, for instance, a matrix normal distribution). The predictors of the dataset are then given by $\{\mathbf{o}_0^i : i \in [1, n]\}$ with $\mathbf{o}_0^i = o\big([\Delta M_1^i]^{-1} M_0^{-1}\big)$, and the labels are simply the transformation matrices M_1^i themselves. See an illustration below [13]:



A meaningful error function of the predicted and actual labels is the sum of the squared geodesic distances:

$$J_g = \sum_{i=1}^{n} \rho^2(f(\mathbf{o}_0^i), \Delta M_1^i).$$

By the Baker-Campbell-Hausdorff formula, we can approximate the geodesic distance between two matrices M_1 and M_2 as

$$\begin{aligned}\rho(M_1, M_2) &= \|\log(M_1^{-1}M_2)\| \\ &= \Big\| \log\Big(\exp\big(-\log(M_1)\big)\exp\big(\log(M_2)\big)\Big)\Big\| \\ &= \big\| \log(M_2) - \log(M_1) + O(|\log(M_1), \log(M_2)|^2)\big\| \\ &\approx \|\log(M_2) - \log(M_1)\|.\end{aligned}$$

Therefore, we can rewrite the error function as the squared difference between the Lie algebras:

$$J_a = \sum_{i=1}^{n} \|\log(f(\mathbf{o}_0^i)) - \log(\Delta M_1^i)\|^2.$$

The approximation is accurate enough because all of the transformations are within a sufficiently small neighborhood of the identity. This motivates reexpressing the regression function as $f(\mathbf{o}) = \exp(g(\mathbf{o}))$. That is, we are now learning a function g which estimates the tangent vector of ΔM_t on its Lie algebra. g must be evaluated in real-time as the object is moving, so it must be relatively simple and fast to evaluate. A reasonable choice is therefore to model g as a linear function, that is,

$$g(\mathbf{o}) = \mathbf{o}^T\Omega,$$

where Ω is a matrix of the appropriate dimensions. Now, let X be the matrix containing the predictors as its rows and Y be the matrix containing vectorized labels as its rows, that is,

$$X = \begin{pmatrix} [\mathbf{o}_0^1]^T \\ \vdots \\ [\mathbf{o}_0^n]^T \end{pmatrix}, \quad Y = \begin{pmatrix} \log(\Delta M_1^1)^T \\ \vdots \\ \log(\Delta M_1^n)^T \end{pmatrix}.$$

Then we equivalently express the error function as

$$J_a = \operatorname{tr}[(X\Omega - Y)(X\Omega - Y)^T].$$

Because we will be updating the regression function in real time, we must keep n low; Tuzel et al suggest $n = 200$. Since the number of data points is smaller than the dimension of the data ($200 < 288$), the solution minimizing the error function will be underdetermined and thus will be prone to overfitting. In order to avoid the overfitting, we add a regularization constant to the loss function, giving us

$$J_r = \operatorname{tr}[(X\Omega - Y)(X\Omega - Y)^T] + \lambda\|\Omega\|^2,$$

for some hyperparameter λ. The minimizer of this loss function can be explicitly expressed as

$$(X^TX + \lambda I)X^TY,$$

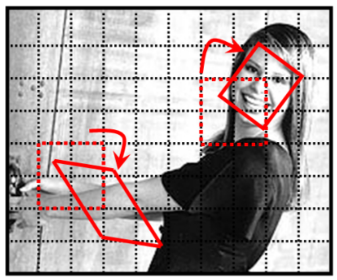
where I is the identity matrix. As the object moves, however, we should update g based on more recent data. To this end, Tuzel et al propose generating $s = 2$ random observations at each time frame according to the same method that the initial dataset was produced. Every $p = 100$ time frames, we aggregate an updated dataset, denoted by X_u and Y_u, consisting of the sp total observations from the last p time frames. Then, letting Ω' denote the previous model parameters and λ and γ be hyperparameters, we update the parameters of the model to minimize the loss

$$J_u = \operatorname{tr}[(X_u\Omega - Y_u)(X_u\Omega - Y_u)^T] + \lambda\|\Omega\|^2 + \gamma\|\Omega - \Omega'\|^2.$$

That is, we now additionally penalize differing from the previous parameters. The minimum is achieved at

$$\Omega = (X_u^T X_u + (\lambda + \gamma)I)^{-1}(X_u^T Y_u + \gamma\Omega').$$

We now address how to identify a particular object in the first place. Suppose we wish to identify a face. Then given a dataset of reference images of faces, we apply random affine transformations $[\Delta M^i]^{-1}$, the logarithms of whose inverses constitute the labels of the dataset, to each image and convert the resulting unit-square areas to orientation histograms, which become the predictors of the dataset. We can, as before, train a linear model on the dataset; however, since this learning can be done offline (as opposed to online, that is, in real time), we are also free to use more complex models. In particular, Tuzel et al propose using bagged trees (see ¡citation¿ for more details). Once such a model is trained, we apply it to a grid of overlapping tiles in the image. We multiply each tile by the predicted transformation matrix and then evaluate the resulting region using an established face detector, such as the Viola and Jones face detector [13]. The following figure [13] illustrates this method:



Acknowledgements

The authors would like to thank Simon Rubinstein-Salzedo and Kishan Jani for their help and support in writing this paper.

References

[1] *Are Strictly Upper Triangular Matrices Nilpotent?*. Stack Exchange, 2013. https://math.stackexchange.com/questions/532372/are-strictly-upper-triangular-matrices-nilpotent/532459#532459.

[2] Andrew J. Baker. *Matrix Groups: An Introduction to Lie Group Theory*. Springer, 2002.

[3] Brian C. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Volume 222 of Graduate Texts in Mathematics. Springer, 2003.

[4] The Bright Side of Mathematics. *Jordan Normal Form, Part 1: Overview*. Youtube, 2020. https://www.youtube.com/watch?v=GVixvieNnyc.

[5] The Bright Side of Mathematics. *Jordan Normal Form, Part 2: An Example*. Youtube, 2020. https://www.youtube.com/watch?v=UKj_ufj1dK4.

[6] The Bright Side of Mathematics. *Jordan Normal Form, Part 4: Transformation Matrix*. Youtube, 2020. https://www.youtube.com/watch?v=KQUgLjcnC8U.

[7] *Chapter 4: Vector Norms and Matrix Norms*. CIS 515, Course at the University of Pennsylvania. 2022. Excerpted from unknown source. *https://www.cis.upenn.edu/ cis515/cis515-11-sl4.pdf*.

[8] *How to get p(A) = 0 without Cayley-Hamilton theorem when A is diagonalizable?*. Stack Exchange, 2011. https://math.stackexchange.com/questions/55724/how-to-get-pa-0-without-cayley-hamilton-theorem-when-a-is-diagonalizable.

[9] Keith Conrad. *Equivalence of Norms*. https://kconrad.math.uconn.edu/blurbs/gradnumthy/equivnorms.pdf

[10] Jonny Evans. *Lie Groups and Lie Algebras*. 10-week-long course at Lancaster University. 2020. http://jde27.uk/lgla/index.html.

[11] Kuo-Chang Chen. *Chapter 8: Introduction to Banach Spaces*. Excerpted from unknown source. https://www.math.nthu.edu.tw/~kchen/teaching/5131week1.pdf.

[12] *Minkowski's Inequality for Sums.* ProofWiki. https://proofwiki.org/wiki/Minkowski%27s_Inequality_for_Sums/Index_2
[13] Oncel Tuzel, Fatih Porikli, Peter Meer. *Learning on Lie Groups for Invariant Detection and Tracking.* IEEE, 2008. https://doi.org/10.1109/CVPR.2008.4587521.
[14] Peter Woit. *Quantum Theory, Groups and Representations: An Introduction.* Springer, 2017.
[15] *Proofs in Linear Algebra via Topology.* Stack Exchange, 2016. https://math.stackexchange.com/questions/1545956/proofs-in-linear-algebra-via-topology/1546538#1546538.
[16] Robin Zhang. *The Baker-Campbell-Hausdorff Formula.* 2017. http://math.columbia.edu/~rzhang/files/BCHFormula.pdf.
[17] Qiang Xu, Dengwu Ma. *Applications of Lie Groups and Lie Algebra to Computer Vision: A Brief Survey.* IEEE, 2012. https://doi.org/10.1109/ICSAI.2012.6223449.