Chapter 4

Matrix Groups

Topics :

- 1. Real and Complex Matrix Groups
- 2. Examples of Matrix Groups
- 3. The Exponential Mapping
- 4. Lie Algebras for Matrix Groups
- 5. More Properties of the Exponential Mapping
- 6. Examples of Lie Algebras of Matrix Groups

Copyright © Claudiu C. Remsing, 2006. All rights reserved.

4.1 Real and Complex Matrix Groups

Throughout, we shall denote by \Bbbk either the *field* \mathbb{R} of real numbers or the *field* \mathbb{C} of complex numbers.

The algebra of $n \times n$ matrices over k

Let \mathbb{k}^m be the set of all *m*-tuples of elements of \mathbb{k} . Under the usual addition and scalar multiplication, \mathbb{k}^m is a vector space over \mathbb{k} . The set $\operatorname{Hom}(\mathbb{k}^n,\mathbb{k}^m)$ of all linear mappings from \mathbb{k}^n to \mathbb{k}^m (i.e., mappings $L:\mathbb{k}^n \to \mathbb{k}^m$ such that $L(\lambda x + \mu y) = \lambda L(x) + \mu L(y)$ for every $x, y \in \mathbb{k}^n$ and $\lambda, \mu \in \mathbb{k}$) is also a vector space over \mathbb{k} .

♦ **Exercise 171** Determine the *dimension* of the vector space $Hom(\Bbbk^n, \Bbbk^m)$.

Let $\mathbb{k}^{m \times n}$ be the set of all $m \times n$ matrices with elements (entries) from \mathbb{k} . It is convenient to *identify*

the *m*-tuple $(a_1, a_2, \dots, a_m) \in \mathbb{k}^m$ with the column *m*-matrix $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \in \mathbb{k}^{m \times 1}.$

♦ **Exercise 172** Give reasons why the *identification* of \mathbb{k}^m with $\mathbb{k}^{m \times 1}$ is legitimate.

Under the usual matrix addition and multiplication, $\mathbb{k}^{m \times n}$ is a vector space over \mathbb{k} . There is a natural one-to-one correspondence

$$A \mapsto L_A (: x \mapsto Ax)$$

between the $m \times n$ matrices with elements from \Bbbk and the linear mappings from \Bbbk^n to \Bbbk^m .

♦ **Exercise 173** Show that the vector spaces $\mathbb{k}^{m \times n}$ and $\mathsf{Hom}(\mathbb{k}^n, \mathbb{k}^m)$ are *isomorphic*. Observe that, in particular, the vector spaces $\mathbb{k}^{1 \times n}$ and $\mathsf{Hom}(\mathbb{k}^n, \mathbb{k}) = (\mathbb{k}^n)^*$ (the *dual* of \mathbb{k}^n) are isomorphic.

NOTE: We do not identify the row n-matrix $\begin{bmatrix} a_1 & a_2 & \dots & a_n \end{bmatrix}$ with the n-tuple (a_1, a_2, \dots, a_n) but rather with the linear mapping (functional)

$$(x_1, x_2, \ldots, x_n) \mapsto a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

Any matrix $A \in \mathbb{k}^{m \times n}$ can be *interpreted* as a linear mapping $L_A \in$ Hom $(\mathbb{k}^n, \mathbb{k}^m)$, whereas any linear mapping $L \in$ Hom $(\mathbb{k}^n, \mathbb{k}^m)$ can be *realized* as a matrix $A \in \mathbb{k}^{m \times n}$. Henceforth we shall not distinguish notationwise between a matrix A and its corresponding linear mapping $x \mapsto Ax$.

NOTE : A matrix (or linear mapping, if one prefers) $A \in \mathbb{k}^{n \times n}$ can be viewed as a vector field (on \mathbb{k}^n) : A associates to each point p in \mathbb{k}^n the tangent vector $A(p) = Ap \in \mathbb{k}^n$. We may think of a *fluid* in motion, so that the velocity of the fluid particles passing through p is always A(p). The vector field is then the current of the *flow* and the paths of the fluid particles are the trajectories. This kind of flow is, of course, very special : A(p) is independent of time, and depends linearly on p.

Notice that $\mathbb{k}^{n \times n}$ is not just a vector space. It also has a multiplication which is associative and distributes over addition (on either side). In other words, under the usual addition and multiplication, $\mathbb{k}^{n \times n}$ is a *ring* (in general not commutative), with identity I_n . Moreover, for all $A, B \in \mathbb{k}^{n \times n}$ and $\lambda \in \mathbb{k}$,

$$\lambda(AB) = (\lambda A)B = A(\lambda B).$$

Such a structure is called an (associative) algebra over k.

 \diamond **Exercise 174** Give the definition of an *algebra* over (the field) k. Write down *all* the axioms.

The topology of $\mathbb{k}^{n \times n}$

For $x \in \mathbb{k}^n$ (= $\mathbb{k}^{n \times 1}$), let

$$||x||_2 := \sqrt{|x_1|^2 + |x_2|^2 + \dots + |x_n|^2}$$

be the 2-norm (or Euclidean norm) on \mathbb{k}^n .

NOTE : For $r \ge 1$, the *r*-norm of $x \in \mathbb{k}^n$ is defined as

$$||x||_r := (|x_1|^r + |x_2|^r + \dots + |x_n|^r)^{1/r}.$$

The following properties hold (for $x, y \in \mathbb{k}^n$ and $\lambda \in \mathbb{k}$):

```
\begin{split} \|x\|_{r} &\geq 0, \quad \text{and} \quad \|x\|_{r} = 0 \iff x = 0 \ ; \\ \|\lambda x\|_{r} &= |\lambda| \, \|x\|_{r} \ ; \\ \|x + y\|_{r} &\leq \|x\|_{r} + \|y\|_{r}. \end{split}
```

In practice, only three of the r-norms are used, and they are :

$$\begin{aligned} \|x\|_{1} &= |x_{1}| + |x_{2}| + \dots + |x_{n}| \quad \text{(the grid norm);} \\ \|x\|_{2} &= \sqrt{|x_{1}|^{2} + |x_{2}|^{2} + \dots + |x_{n}|^{2}} \quad \text{(the Euclidean norm);} \\ \|x\|_{\infty} &= \lim_{r \to \infty} \|x\|_{r} &= \max\{|x_{1}|, |x_{2}|, \dots, |x_{n}|\} \quad \text{(the max norm).} \end{aligned}$$

For $x \in \mathbb{k}^n$, we have

$$||x||_{\infty} \le ||x||_{2} \le ||x||_{1} \le \sqrt{n} \cdot ||x||_{2} \le n \cdot ||x||_{\infty}$$

and so any two of these norms are *equivalent* (i.e., the associated metric topologies are identical). In fact, all norms on a finite dimensional vector space (over \Bbbk) are equivalent.

The metric topology *induced* by (the Euclidean distance)

$$(x,y) \mapsto \|x-y\|_2$$

is the *natural topology* on the set (vector space) \mathbb{k}^n .

 \diamond **Exercise 175** Show that, for $x, y \in \mathbb{k}^n$,

$$|||x||_2 - ||y||_2| \le ||x - y||_2.$$

Hence deduce that the function

$$\|\cdot\|_2: \mathbb{k}^n \to \mathbb{R}, \quad x \mapsto \|x\|_2$$

is *continuous* (with respect to the natural topologies on \mathbb{k}^n and \mathbb{R}).

♦ **Exercise 176** Given $A \in \mathbb{k}^{n \times n}$, show that the linear mapping (on \mathbb{k}^n) $x \mapsto Ax$ is *continuous* (with respect to the natural topology on \mathbb{k}^n).

Let $A \in \mathbb{k}^{n \times n}$. The 2-norm $\|\cdot\|_2$ on $\mathbb{k}^{n \times 1}$ induces a (matrix) norm on $\mathbb{k}^{n \times n}$ by setting

$$||A|| := \max_{||x||_2=1} ||Ax||_2.$$

The subset $K = \{x \in \mathbb{k}^n \mid ||x||_2 = 1\} \subset \mathbb{k}^n$ is closed and bounded, and so is *compact*. [A subset of the metric space \mathbb{k}^n is compact if and only if it is closed and bounded.] On the other hand, the function $f : K \to \mathbb{R}, \quad x \mapsto ||Ax||_2$ is *continuous*. [The composition of two continuous maps is a continuous map.] Hence the maximum value $\max_{x \in K} ||Ax||_2$ must exist.

NOTE: The following topological result holds: If $K \subset \mathbb{k}^n$ is a (nonempty) compact set, then any continuous function $f : K \to \mathbb{R}$ is bounded; that is, the image set $f(K) = \{f(x) | x \in K\} \subseteq \mathbb{R}$ is bounded. Moreover, f has a global maximum (and a global minimum).

♦ **Exercise 177** Show that the induced norm $\|\cdot\|$ is *compatible* with its underlying norm $\|\cdot\|_2$; that is (for $A \in \mathbb{k}^{n \times n}$ and $x \in \mathbb{k}^n$),

$$||Ax||_2 \le ||A|| \, ||x||_2.$$

 $\|\cdot\|$ is a *matrix norm* on $\mathbb{k}^{n \times n}$, called the **operator norm**; that is, it has the following four properties (for $A, B \in \mathbb{k}^{n \times n}$ and $\lambda \in \mathbb{k}$):

- (MN1) $||A|| \ge 0$, and $||A|| = 0 \iff A = 0$;
- (MN2) $\|\lambda A\| = |\lambda| \|A\|$;
- (MN3) $||A + B|| \le ||A|| + ||B||;$
- (MN4) $||AB|| \le ||A|| ||B||.$

NOTE : There is a simple procedure (well-known in numerical linear algebra) for calculating the operator norm of an $n \times n$ matrix A. This is

$$||A|| = \sqrt{\lambda_{\max}},$$

where λ_{\max} is the largest eigenvalue of the matrix A^*A . Here A^* denotes the *Hermitian conjugate* (i.e., the conjugate transpose) matrix of A; in the case $\mathbb{k} = \mathbb{R}$, $A^* = A^{\top}$.

We define a *metric* ρ on (the algebra) $\mathbb{k}^{n \times n}$ by

$$\rho(A, B) := \|A - B\|.$$

Associated to this metric is a natural *topology* on $\mathbb{k}^{n \times n}$. Hence fundamental topological concepts, like *open sets, closed sets, compactness, connectedness,* as well as *continuity*, can be introduced. In particular, we can speak of continuous functions from $\mathbb{k}^{n \times n}$ into \mathbb{k} .

♦ **Exercise 178** For $1 \le i, j \le n$, show that the coordinate function

$$\operatorname{coord}_{ii} : \mathbb{k}^{n \times n} \to \mathbb{k}, \quad A \mapsto a_{ii}$$

is continuous. [HINT : Show first that $|a_{ij}| \leq ||A||$ and then verify the defining condition for continuity.]

It follows immediately that if $f : \mathbb{k}^{n^2} \to \mathbb{k}$ is continuous, then the associated function

$$\widetilde{f} = f \circ (\operatorname{coord}_{ij}) : \mathbb{k}^{n \times n} \to \mathbb{k}, \quad A \mapsto f((a_{ij}))$$

is also continuous. Here $(a_{ij}) = (a_{11}, a_{12}, \dots, a_{1n}, a_{21}, \dots, a_{nn}) \in \mathbb{k}^{n^2}$.

 \diamond **Exercise 179** Show that the *determinant function*

$$\det : \mathbb{k}^{n \times n} \to \mathbb{k}, \quad A \mapsto \det A := \sum_{\sigma \in S_n} (-1)^{|\sigma|} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

and the trace function

$$\operatorname{tr}: \mathbb{k}^{n \times n} \to \mathbb{k}, \quad A \mapsto \operatorname{tr} A := \sum_{i=1}^{n} a_{ii}$$

are continuous.

The metric space $(\mathbb{k}^{n \times n}, \rho)$ is complete. This means that every Cauchy sequence $(A_r)_{r \ge 0}$ in $\mathbb{k}^{n \times n}$ has a unique limit $\lim_{r \to \infty} A_r$. Furthermore,

$$\left(\lim_{r\to\infty}A_r\right)_{ij}=\lim_{r\to\infty}(A_r)_{ij}.$$

Indeed, the limit on the RHS exists, so it is sufficient to check that the required matrix limit is the matrix A with $a_{ij} = \lim_{r \to \infty} (A_r)_{ij}$. The sequence $(A_r - A)_{r \ge 0}$ satisfies

$$||A_r - A|| \le \sum_{i,j=1}^n |(A_r)_{ij} - a_{ij}| \to 0 \text{ as } r \to \infty$$

and so $A_r \to A$.

Groups of matrices

Let $\mathsf{GL}(n, \Bbbk)$ be the set of all invertible $n \times n$ matrices over \Bbbk (or, equivalently, the set of all linear transformations on \Bbbk^n). So

$$\mathsf{GL}(n,\mathbb{k}) := \{ A \in \mathbb{k}^{n \times n} \, | \, \det A \neq 0 \}.$$

♦ **Exercise 180** Verify that the set GL(n, k) is a *group* under matrix multiplication.

 $\mathsf{GL}(n, \Bbbk)$ is called the **general linear group** over \Bbbk . We will refer to $\mathsf{GL}(n, \mathbb{R})$ and $\mathsf{GL}(n, \mathbb{C})$ as the *real* and *complex* general linear group, respectively.

A 1×1 matrix over k is just an element of k and matrix multiplication of two such elements is just multiplication in k. So we see that

 $\mathsf{GL}(1,\mathbb{k}) = \mathbb{k}^{\times}$ (the multiplicative group of $\mathbb{k} \setminus \{0\}$).

4.1.1 PROPOSITION. GL (n, \mathbb{k}) is an open subset of $\mathbb{k}^{n \times n}$.

PROOF : We have seen that the function det : $\mathbb{k}^{n \times n} \to \mathbb{k}$ is continuous (see **Exercise 179**). Then observe that

$$\mathsf{GL}(n,\mathbb{k}) = \mathbb{k}^{n \times n} \setminus \det^{-1}(0).$$

Since the set $\{0\}$ is closed (in \Bbbk), it follows that $\det^{-1}(0) = \det^{-1}(\{0\}) \subset \Bbbk^{n \times n}$ is also closed. [The preimage of a closed set under a continuous map is a closed set.] Hence $\mathsf{GL}(n, \Bbbk)$ is open. [The complement of a closed set is an open set.]

Let G be a subgroup of the general linear group $\mathsf{GL}(n, \Bbbk)$. If G is also a closed subspace of $\mathsf{GL}(n, \Bbbk)$, we say that G is a *closed* subgroup.

4.1.2 DEFINITION. A closed subgroup of $GL(n, \mathbb{k})$ is called a **matrix group** over \mathbb{k} (or a **matrix subgroup** of $GL(n, \mathbb{k})$).

Matrix groups are also known as *linear* groups or even as *matrix Lie* groups. This latter terminology emphasizes the remarkable fact that *every* matrix group is a Lie group.

NOTE : The condition that the group of matrices $G \subseteq \mathsf{GL}(n, \Bbbk)$ is a closed subset of (the metric space) $\mathsf{GL}(n, \Bbbk)$ means that the following condition is satisfied : *if* $(A_r)_{r\geq 0}$ is any sequence of matrices in G and $A_r \to A$, then either $A \in G$ or A is not invertible (i.e. $A \notin \mathsf{GL}(n, \Bbbk)$).

The condition that G be a *closed* subgroup, as opposed to merely a subgroup, should be regarded as a "technicality" since most of the *interesting* subgroups of $GL(n, \Bbbk)$ have this property. Almost all of the matrix groups we will consider have the stronger property that if $(A_r)_{r\geq 0}$ is any sequence of matrices in G converging to some matrix A, then $A \in G$.

We will often use the notation $G \leq \mathsf{GL}(n, \Bbbk)$ to indicate that G is a (matrix) subgroup of $\mathsf{GL}(n, \Bbbk)$.

4.1.3 EXAMPLE. The general linear group $GL(n, \mathbb{k})$ is a matrix group (over \mathbb{k}).

4.1.4 EXAMPLE. An example of a group of matrices which is *not* a matrix group is the set of all $n \times n$ invertible matrices all of whose entries are rational numbers. This is in fact a subgroup of $\mathsf{GL}(n,\mathbb{C})$ but not a closed subgroup; that is, one can (easily) have a sequence of invertible matrices with rational entries converging to an invertible matrix with some irrational entries.

\diamond **Exercise 181** * Let $a \in \mathbb{R} \setminus \mathbb{Q}$. Show that

$$G = \left\{ \begin{bmatrix} e^{it} & 0\\ 0 & e^{iat} \end{bmatrix} \mid t \in \mathbb{R} \right\}$$

is a subgroup of $\mathsf{GL}(2,\mathbb{C})$, and then find a sequence of matrices in G which converges to $-I_2 \notin G$. This means that G is *not* a matrix group. [HINT : By taking $t = (2n+1)\pi$ for a suitably chosen $n \in \mathbb{Z}$, we can make *ta arbitrarily close* to an odd integer multiple of π , $(2m+1)\pi$ say. It is sufficient to show that for any positive integer N, there exist $n, m \in \mathbb{Z}$ such that $|(2n+1)a - (2m+1)| < \frac{1}{N} \cdot |$

NOTE : The *closure* of G (in $\mathsf{GL}(2,\mathbb{C})$) can be thought of as (the direct product) $\mathbb{S}^1 \times \mathbb{S}^1$ and so *is* a matrix group (see **Exercise 195**).

4.1.5 PROPOSITION. Let G be a matrix group over \Bbbk and H a closed subgroup of G. Then H is a matrix group over \Bbbk .

PROOF : Every sequence $(A_r)_{r\geq 0}$ in H with a limit in $\mathsf{GL}(n, \Bbbk)$ actually has its limit in G since each $A_r \in H \subseteq G$ and G is closed in $\mathsf{GL}(n, \Bbbk)$. Since H is closed in G, this means that $(A_r)_{r\geq 0}$ has a limit in H. So H is closed in $\mathsf{GL}(n, \Bbbk)$, showing it is a matrix group over \Bbbk .

 \diamond **Exercise 182** Prove that any *intersection* of matrix groups (over \Bbbk) is a matrix group.

4.1.6 EXAMPLE. Denote by $SL(n, \mathbb{k})$ the set of all $n \times n$ matrices over \mathbb{k} , having determinant one. So

$$\mathsf{SL}(n,\Bbbk) := \{A \in \Bbbk^{n \times n} \mid \det A = 1\} \subseteq \mathsf{GL}(n,\Bbbk).$$

♦ **Exercise 183** Show that $SL(n, \Bbbk)$ is a closed subgroup of $GL(n, \Bbbk)$ and hence is a matrix group over \Bbbk .

 $\mathsf{SL}(n, \Bbbk)$ is called the **special linear group** over \Bbbk . We will refer to $\mathsf{SL}(n, \mathbb{R})$ and $\mathsf{SL}(n, \mathbb{C})$ as the *real* and *complex* special linear groups, respectively.

4.1.7 DEFINITION. A closed subgroup of a matrix group G is called a **matrix subgroup** of G.

4.1.8 EXAMPLE. We can consider $\mathsf{GL}(n, \Bbbk)$ as a subgroup of $\mathsf{GL}(n+1, \Bbbk)$ by *identifying* the $n \times n$ matrix $A = \begin{bmatrix} a_{ij} \end{bmatrix}$ with

$$\begin{bmatrix} 1 & 0 \\ 0 & A \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & a_{11} & \dots & a_{1n} \\ 0 & a_{21} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & a_{n1} & \dots & a_{nn} \end{bmatrix}.$$

It is easy to verify that $\mathsf{GL}(n, \Bbbk)$ is closed in $\mathsf{GL}(n+1, \Bbbk)$ and hence $\mathsf{GL}(n, \Bbbk)$ is a matrix subgroup of $\mathsf{GL}(n+1, \Bbbk)$.

♦ **Exercise 184** Show that $SL(n, \Bbbk)$ is a matrix subgroup of $SL(n+1, \Bbbk)$.

4.2 Examples of Matrix Groups

The vector space $\mathbb{k}^{n \times n}$ over \mathbb{k} can be considered to be a *real* vector space, of dimension n^2 or $2n^2$, respectively. Explicitly, $\mathbb{R}^{n \times n}$ is (isomorphic to) \mathbb{R}^{n^2} , and $\mathbb{C}^{n \times n}$ is (isomorphic to) $\mathbb{C}^{n^2} = \mathbb{R}^{2n^2}$. Hence we may assume, without any loss of generality, that $\mathbb{k}^{n \times n}$ is some Euclidean space \mathbb{R}^m .

The real general linear group $GL(n, \mathbb{R})$

We showed that $\mathsf{GL}(n,\mathbb{R})$ is a matrix group and that it is an *open* subset of the vector space $\mathbb{R}^{n \times n} (= \mathbb{R}^{n^2})$. Since the set $\mathsf{GL}(n,\mathbb{R})$ is not closed, it is *not* compact. [Any compact set is a closed set.]

The determinant function det : $\mathsf{GL}(n,\mathbb{R}) \to \mathbb{R}$ is continuous (in fact, *smooth*) and maps $\mathsf{GL}(n,\mathbb{R})$ onto the two *components* of \mathbb{R}^{\times} . Thus $\mathsf{GL}(n,\mathbb{R})$ is *not* connected. [The image of a connected set under a continuous map is a connected set.]

NOTE : A matrix group G is said to be **connected** if given any two matrices $A, B \in G$, there exists a continuous path $\gamma : [a, b] \to G$ with $\gamma(a) = A$ and $\gamma(b) = B$. This property is what is called **path-connectedness** in topology, which is not (in general) the same as connectedness. However, it is a fact (not particularly obvious at the moment) that a matrix group is connected if and only if it is path-connected. So in a slight abuse of terminology we shall continue to refer to the above property as connectedness.

A matrix group G which is not connected can be decomposed (uniquely) as a union of several pieces, called *components*, such that two elements of the same component can be joined by a continuous path, but two elements of different components cannot. The component of G containing the identity is a closed subgroup of G (and hence a connected matrix group).

Consider the sets

$$\begin{aligned} \mathsf{GL}^+\left(n,\mathbb{R}\right) &:= & \{A\in\mathsf{GL}\left(n,\mathbb{R}\right) | \det A > 0\} \\ \mathsf{GL}^-\left(n,\mathbb{R}\right) &:= & \{B\in\mathsf{GL}\left(n,\mathbb{R}\right) | \det B < 0\}. \end{aligned}$$

These two disjoint subsets of $GL(n, \mathbb{R})$ are open and such that

 $\mathsf{GL}^{+}(n,\mathbb{R}) \cup \mathsf{GL}^{-}(n,\mathbb{R}) = \mathsf{GL}(n,\mathbb{R}).$

[The preimage of an open set under a continuous map is an open set.]

♦ **Exercise 185** Show that $\mathsf{GL}^+(n, \mathbb{R})$ is a matrix subgroup of $\mathsf{GL}(n, \mathbb{R})$ but $\mathsf{GL}^-(n, \mathbb{R})$ is not.

The mapping

$$A \in \mathsf{GL}^+(n,\mathbb{R}) \mapsto SA \in \mathsf{GL}^-(n,\mathbb{R})$$

where $S = \text{diag}(1, 1, \dots, 1, -1)$, is a bijection (in fact, a *diffeomorphism*). The transformation $x \mapsto Sx$ may be thought of as a *reflection* in the hyperplane $\mathbb{R}^{n-1} = \mathbb{R}^{n-1} \times \{0\} \subset \mathbb{R}^n$.

NOTE : The group $\mathsf{GL}^+(n,\mathbb{R})$ is connected, which proves that $\mathsf{GL}^+(n,\mathbb{R})$ is the connected component of the identity in $\mathsf{GL}(n,\mathbb{R})$ and that $\mathsf{GL}(n,\mathbb{R})$ has two (connected) components.

The real special linear group $SL(n, \mathbb{R})$

Recall that

$$SL(n, \mathbb{R}) := \{A \in GL(n, \mathbb{R}) | \det A = 1\} = \det^{-1}(1).$$

It follows that $SL(n, \mathbb{R})$ is a closed subgroup of $GL(n, \mathbb{R})$ and hence is a matrix group. [The preimage of a closed set under a continuous map is a closed set.] We introduce a new matrix norm on $\mathbb{R}^{n \times n}$, called the *Frobenius* norm, as follows :

$$||A||_F := \sqrt{\operatorname{tr}(A^{\top}A)} = \sqrt{\sum_{i,j=1}^n a_{ij}^2}.$$

NOTE : The Frobenius norm coincides with the Euclidean norm on \mathbb{R}^{n^2} , and is much easier to compute than the operator norm. However, *all* matrix norms on $\mathbb{R}^{n \times n}$ are *equivalent* (i.e., they generate the same metric topology).

We shall use this (matrix) norm to show that $\mathsf{SL}(n,\mathbb{R})$ is *not* compact. Indeed, all matrices of the form

 $\begin{bmatrix} 1 & 0 & \dots & t \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$

are elements of $\mathsf{SL}(n,\mathbb{R})$ whose norm equals $\sqrt{n+t^2}$ for any $t \in \mathbb{R}$. Thus $\mathsf{SL}(n,\mathbb{R})$ is *not* a bounded subset of $\mathbb{R}^{n \times n}$ and hence is *not* compact. [In a metric space, any compact set is bounded.]

NOTE : The special linear group $SL(n, \mathbb{R})$ is connected.

More on $SL(2,\mathbb{R})$.

The orthogonal and special orthogonal groups O(n) and SO(n)

The set

$$\mathsf{O}(n) := \{ A \in \mathbb{R}^{n \times n} \, | \, A^\top A = I_n \}$$

is the **orthogonal group**. Clearly, every orthogonal matrix $A \in O(n)$ has an inverse, namely A^{\top} . Hence $O(n) \subseteq GL(n, \mathbb{R})$.

♦ **Exercise 186** Verify that O(n) is a *subgroup* of the general linear group $GL(n, \mathbb{R})$.

The single matrix equation $A^{\top}A = I_n$ is equivalent to n^2 equations for the n^2 real numbers a_{ij} , i, j = 1, 2, ..., n:

$$\sum_{k=1}^{n} a_{ki} a_{kj} = \delta_{ij}.$$

This means that O(n) is a *closed* subset of $\mathbb{R}^{n \times n}$ and hence of $GL(n, \mathbb{R})$.

♦ **Exercise 187** Prove that O(n) is a closed subset of \mathbb{R}^{n^2} .

Thus O(n) is a matrix group. The group O(n) is also bounded in $\mathbb{R}^{n \times n}$. Indeed, the (Frobenius) norm of $A \in O(n)$ is

$$||A||_F = \sqrt{\operatorname{tr}(A^{\top}A)} = \sqrt{\operatorname{tr}I_n} = \sqrt{n}.$$

Hence the group O(n) is *compact*. [A subset of $\mathbb{R}^{n \times n}$ is compact if and only if it is closed and bounded.]

Let us consider the determinant function (restricted to O(n)), det : $O(n) \rightarrow \mathbb{R}^{\times}$. Then for $A \in O(n)$

$$\det I_n = \det (A^{\top}A) = \det A^{\top} \cdot \det A = (\det A)^2.$$

Hence det $A = \pm 1$. So we have

$$\mathsf{O}(n) = \mathsf{O}^+(n) \cup \mathsf{O}^-(n)$$

where

$$O^{+}(n) := \{A \in O(n) | \det A = 1\}$$
 and $O^{-}(n) := \{A \in O(n) | \det A = -1\}.$

NOTE: The group $O^+(n)$ is connected, which proves that $O^+(n)$ is the connected component of the identity in O(n).

The **special orthogonal group** is defined as

$$\mathsf{SO}(n) := \mathsf{O}(n) \cap \mathsf{SL}(n,\mathbb{R}).$$

That is,

$$SO(n) = \{A \in O(n) | \det A = 1\} = O^+(n).$$

It follows that SO(n) is a closed subset of O(n) and hence is *compact*. [A closed subset of a compact set is compact.]

NOTE : One of the main reasons for the study of these groups O(n), SO(n) is their relationship with *isometries* (i.e., distance-preserving transformations on the Euclidean space \mathbb{R}^n). If such an isometry fixes the origin, then it is actually a linear transformation and so – with respect to the standard basis – corresponds to a matrix A. The isometry condition is equivalent to the fact that (for all $x, y \in \mathbb{R}^n$)

$$Ax \bullet Ay = x \bullet y,$$

which in turn is equivalent to the condition that $A^{\top}A = I_n$ (i.e., A is orthogonal). Elements of SO(n) are (identified with) *rotations* (or direct isometries); elements of $O^-(n)$ are sometimes referred to as indirect isometries.

The Lorentz group Lor(1, n)

Consider the inner-product (i.e., nondegenerate symmetric bilinear form) \odot on (the vector space) \mathbb{R}^{n+1} given by (for $x, y \in \mathbb{R}^{n+1}$)

$$x \odot y := -x_1 y_1 + \sum_{i=2}^{n+1} x_i y_i$$

(the so-called *Minkowski product*). It is standard to denote this inner-product space by $\mathbb{R}^{1,n}$.

 \diamond **Exercise 188** Show that the group of all linear isometries (i.e., linear transformations on $\mathbb{R}^{1,n}$ that preserve the Minkowski product) is *isomorphic* to the matrix group

$$\mathsf{O}(1,n) := \left\{ A \in \mathsf{GL}(n+1,\mathbb{R}) \,|\, A^{\top}SA = S \right\}$$

where

$$S = \operatorname{diag}\left(-1, 1, 1, \dots, 1\right) = \begin{bmatrix} -1 & 0\\ 0 & I_n \end{bmatrix} \in \operatorname{\mathsf{GL}}(n+1, \mathbb{R}).$$

In a similar fashion, one can define more general matrix groups

$$\mathsf{O}(k,\ell) \leq \mathsf{GL}(k+\ell,\mathbb{R}) \text{ and } \mathsf{SO}(k,\ell) \leq \mathsf{SL}(k+\ell,\mathbb{R})$$

usually called "pseudo-orthogonal" groups.

♦ **Exercise 189** Define the inner-product $\langle \cdot, \cdot \rangle_{k,\ell}$ on $\mathbb{R}^{k+\ell}$ by the formula

$$\langle x, y \rangle_{k,\ell} := -x_1 y_1 - \dots - x_k y_k + x_{k+1} y_{k+1} + \dots + x_{k+\ell} y_{k+\ell}.$$

The pseudo-orthogonal group $O(k, \ell)$ consists of all matrices $A \in GL(k+\ell, \mathbb{R})$ which preserve this inner-product (i.e., such that $\langle Ax, Ay \rangle_{k,\ell} = \langle x, y \rangle_{k,\ell}$ for all $x, y \in \mathbb{R}^{k+\ell}$).

(a) Verify that $O(k, \ell)$ is a *matrix subgroup* of $GL(k + \ell, \mathbb{R})$.

(b) Let

$$Q = \operatorname{diag}\left(-1, \dots, -1, 1, \dots, 1\right) = \begin{bmatrix} -I_k & 0\\ 0 & I_\ell \end{bmatrix}$$

Prove that a matrix $A \in \mathsf{GL}(k+\ell, \mathbb{R})$ is in $\mathsf{O}(k, \ell)$ if and only if $A^{\top}QA = Q$. Hence deduce that det $A = \pm 1$.

(c) Verify that $SO(k, \ell) := O(k, \ell) \cap SL(k + \ell, \mathbb{R})$ is a matrix subgroup of $SL(k + \ell, \mathbb{R})$.

NOTE : Since $O(k, \ell)$ and $O(\ell, k)$ are essentially the same group, we may assume (without any loss of generality) that $1 \le k \le \ell$. The pseudo-orthogonal groups are neither compact nor connected. The groups $O(k, \ell)$ have four (connected) components, whereas $SO(k, \ell)$ have two components.

For each positive number $\rho > 0$, the hyperboloid

$$\mathcal{H}_{1,n}(\rho) := \left\{ x \in \mathbb{R}^{1,n} \, | \, \langle x, x \rangle = -\rho \right\}$$

has two (connected) components

$$\mathcal{H}_{1,n}^+(\rho) = \{ x \in \mathcal{H}_{1,n}(\rho) \, | \, x_1 > 0 \} \quad \text{and} \quad \mathcal{H}_{1,n}^-(\rho) = \{ x \in \mathcal{H}_{1,n}(\rho) \, | \, x_1 < 0 \} \,.$$

We define the **Lorentz group** Lor(1, n) to be the (closed) subgroup of SO(1, n) preserving each of the connected sets $\mathcal{H}_{1,n}^{\pm}(1)$. Thus

$$\operatorname{Lor}(1,n) := \left\{ A \in \operatorname{SO}(1,n) \, | \, A\mathcal{H}_{1,n}^{\pm}(1) = \mathcal{H}_{1,n}^{\pm}(1) \right\} \le \operatorname{SO}(1,n).$$

It turns out that $A \in \text{Lor}(1, n)$ if and only if it preserves the hyperboloids $\mathcal{H}_{1,n}^{\pm}(\rho), \ \rho > 0$ and the "light cones" $\mathcal{H}_{1,n}^{\pm}(0)$.

NOTE : The Lorentz group Lor(1, n) is connected.

Of particular interest in physics is the Lorentz group Lor = Lor(1,3). That is,

$$\mathsf{Lor} = \left\{ L \in \mathsf{SO}(1,3) \, | \, L\mathcal{H}_{1,3}^{\pm}(\rho) = \mathcal{H}_{1,3}^{\pm}(\rho), \ \rho \ge 0 \right\} \le \mathsf{SO}(1,3).$$

 \diamond **Exercise 190** Show that

(a) The matrix
$$A = \begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix}$$
 is in SO(1,1).

(b) For every $s, t \in \mathbb{R}$

 $\begin{bmatrix} \cosh s & \sinh s \\ \sinh s & \cosh s \end{bmatrix} \begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix} = \begin{bmatrix} \cosh(s+t) & \sinh(s+t) \\ \sinh(s+t) & \cosh(s+t) \end{bmatrix}.$

(c) Every element (matrix) of O(1,1) can be written in one of the four forms

$$\begin{bmatrix} \cosh t & \sinh t \\ \sinh t & \cosh t \end{bmatrix}, \begin{bmatrix} -\cosh t & \sinh t \\ \sinh t & -\cosh t \end{bmatrix}, \begin{bmatrix} \cosh t & -\sinh t \\ \sinh t & -\cosh t \end{bmatrix}, \begin{bmatrix} \cosh t & -\sinh t \\ \sinh t & \cosh t \end{bmatrix}, \begin{bmatrix} -\cosh t & -\sinh t \\ \sinh t & \cosh t \end{bmatrix}$$

(Since $\cosh t$ is always positive, there is no overlap among the four cases. Matrices of the first two forms have determinant one; matrices of the last two forms have determinant minus one.)

NOTE : We can write

$$\begin{array}{rcl} \mathsf{SO}\left(1,1\right) &=& \mathsf{Lor}\left(1,1\right) \cup \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \mathsf{Lor}\left(1,1\right) \\ \mathsf{O}\left(1,1\right) &=& \mathsf{SO}\left(1,1\right) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \mathsf{SO}\left(1,1\right). \end{array}$$

More on Lor (1,2).....

The real symplectic group $Sp(2n, \mathbb{R})$

Let

$$\mathbb{J} := \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in \mathsf{SL}(2n, \mathbb{R}).$$

A matrix $A \in \mathbb{R}^{2n \times 2n}$ is called *symplectic* if

$$A^{\top} \mathbb{J} A = \mathbb{J}.$$

NOTE: The word *symplectic* was invented by HERMANN WEYL (1885-1955), who substituted Greek for Latin roots in the word *complex* to obtain a term which would describe a group (related to "line complexes" but which would not be confused with complex numbers).

Let $\mathsf{Sp}(2n,\mathbb{R})$ be the set of all $2n \times 2n$ symplectic matrices. Taking determinants of the condition $A^{\top} \mathbb{J}A = \mathbb{J}$ gives

$$1 = \det \mathbb{J} = (\det A^{\top}) \cdot (\det \mathbb{J}) \cdot (\det A) = (\det A)^2.$$

Hence det $A = \pm 1$, and so $A \in \mathsf{GL}(2n, \mathbb{R})$. Furthermore, if $A, B \in \mathsf{Sp}(2n, \mathbb{R})$, then

$$(AB)^{\top} \mathbb{J}(AB) = B^{\top} A^{\top} \mathbb{J}AB = \mathbb{J}.$$

Hence $AB \in \mathsf{Sp}(2n, \mathbb{R})$. Now, if $A^{\top} \mathbb{J}A = \mathbb{J}$, then

$$\mathbb{J}A = (A^\top)^{-1}\mathbb{J} = (A^{-1})^\top \mathbb{J}$$

 \mathbf{SO}

$$\mathbb{J} = (A^{-1})^\top \mathbb{J} A^{-1}.$$

It follows that $A^{-1} \in \mathsf{Sp}(2n, \mathbb{R})$ and hence $\mathsf{Sp}(2n, \mathbb{R})$ is a group. In fact, it is a *closed* subgroup of $\mathsf{GL}(2n, \mathbb{R})$, and thus a matrix group.

NOTE : The symplectic group $Sp(2n, \mathbb{R})$ is *connected*. (It turns out that the determinant of a symplectic matrix must be positive; this fact is by no means obvious.

♦ **Exercise 191** Check that $\mathsf{Sp}(2, \mathbb{R}) = \mathsf{SL}(2, \mathbb{R})$. (In general, it is *not* true that $\mathsf{Sp}(2n, \mathbb{R}) = \mathsf{SL}(2n, \mathbb{R})$.)

 $\diamond \text{ Exercise 192 Given } A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathsf{GL}(2n, \mathbb{R}), \text{ show that } A \in \mathsf{Sp}(2n, \mathbb{R}) \text{ if}$ and only if $a^{\top}c$ and $b^{\top}d$ are symmetric and $a^{\top}d - c^{\top}b = I_n$.

All matrices of the form

$$\begin{bmatrix} I_n & 0\\ tI_n & I_n \end{bmatrix}$$

are symplectic. However, the (Frobenius) norm of such a matrix is equal to $\sqrt{2n+t^2n}$, which is *unbounded* if $t \in \mathbb{R}$. Therefore, $\mathsf{Sp}(2n,\mathbb{R})$ is not a bounded subset of $\mathbb{R}^{2n \times 2n}$ and hence is *not* compact.

 \diamond **Exercise 193** Consider the skew-symmetric bilinear form on (the vector space) \mathbb{R}^{2n} defined by

$$\Omega(x,y) := \sum_{i=1}^{n} (x_i y_{n+i} - x_{n+i} y_i)$$

(the standard symplectic form or the "canonical" symplectic structure). Show that a linear transformation (on \mathbb{R}^{2n}) $x \mapsto Ax$ preserves the symplectic form Ω if and only if $A^{\top} \mathbb{J}A = \mathbb{J}$ (i.e., the matrix A is symplectic). Such a structure-preserving transformation is called a symplectic transformation.

The group of all symplectic transformations on \mathbb{R}^{2n} (equipped with the symplectic form Ω) is *isomorphic* to (the matrix group) $\mathsf{Sp}(2n,\mathbb{R})$.

NOTE: The symplectic group is related to *classical mechanics*. Consider a particle of mass m moving in a *potential field* V. Newton's second law states that the particle moves along a curve $t \mapsto x(t)$ in in Cartesian 3-space \mathbb{R}^3 in such a way that $m\ddot{x} = -\text{grad } V(x)$. Introduce the conjugate momenta $p_i = m\dot{x}_i$, i = 1, 2, 3 and the energy (Hamiltonian)

$$H(x,p) := \frac{1}{2m} \sum_{i=1}^{3} p_i^2 + V(x).$$

Then

$$\frac{\partial H}{\partial x_i} = \frac{\partial V}{\partial x_i} = -m\ddot{x}_i = -\dot{p}_i \quad \text{and} \quad \frac{\partial H}{\partial p_i} = \frac{1}{m}p_i = \dot{x}_i$$

and hence Newton's law $\mathbf{F} = m a$ is equivalent to Hamilton's equations

$$\dot{x}_i = \frac{\partial H}{\partial p_i}$$
 and $\dot{p}_i = -\frac{\partial H}{\partial x_i}$ $(i = 1, 2, 3).$

Writing z = (x, p),

$$\mathbb{J} \cdot \operatorname{grad} H(z) = \begin{bmatrix} 0 & I_3 \\ -I_3 & 0 \end{bmatrix} \begin{bmatrix} \frac{\partial H}{\partial x} \\ \\ \frac{\partial H}{\partial p} \end{bmatrix} = (\dot{x}, \dot{p}) = \dot{z}$$

so Hamilton equations read $\dot{z} = \mathbb{J} \cdot \operatorname{grad} H(z)$. Now let

$$F: \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3 \times \mathbb{R}^3$$

and write w(t) = F(z(t)). If z(t) satisfies Hamilton's equations

$$\dot{z} = \mathbb{J} \cdot \operatorname{grad} H(z)$$

then w(t) = F(z(t)) satisfies $\dot{w} = A^{\top}\dot{z}$, where $A^{\top} = [\partial w^i/\partial z^j]$ is the Jacobian matrix of f. By the chain rule,

$$\dot{w} = A^{\top} \mathbb{J}\operatorname{grad}_{z} H(z) = A^{\top} \mathbb{J}A\operatorname{grad}_{w} H(z(w)).$$

Thus, the equations for w(t) have the form of Hamilton's equations with energy K(w) = H(z(w)) if and only if $A^{\top} \mathbb{J}A = \mathbb{J}$; that is, if and only if A is symplectic. A nonlinear transformation F is *canonical* if and only if its Jacobian matrix is symplectic (or, if one prefers, its tangent mapping is a symplectic transformation).

As a special case, consider a (linear transformation) $A \in \text{Sp}(2n, \mathbb{R})$ and let w = Az. Suppose H is quadratic (i.e., of the form $H(z) = \frac{1}{2}z^{\top}Bz$ where B is a symmetric matrix). Then grad H(z) = Bz and thus the equations of motion become the linear equations $\dot{z} = \mathbb{J}Bz$. Now

$$\dot{w} = A\dot{z} = A\mathbb{J}Bz = \mathbb{J}(A^{\top})^{-1}Bz = \mathbb{J}(A^{\top})^{-1}BA^{-1}Az = \mathbb{J}B'w$$

where $B' = (A^{\top})^{-1}BA^{-1}$ is symmetric. For the new Hamiltonian we get

$$H'(w) = \frac{1}{2}w^{\top}(A^{\top})^{-1}BA^{-1}w = \frac{1}{2}(A^{-1}w)^{\top}BA^{-1}w$$
$$= H(A^{-1}w) = H(z).$$

Thus $\mathsf{Sp}(2n,\mathbb{R})$ is the linear invariance group of classical mechanics.

The complex general linear group $GL(n, \mathbb{C})$

Many important matrix groups involve *complex* matrices. As in the real case,

$$\mathsf{GL}(n,\mathbb{C}):=\{A\in\mathbb{C}^{n\times n}\,|\,\det A\neq 0\}$$

is an *open* subset of $\mathbb{C}^{n \times n}$, and hence is *not* compact. Clearly $\mathsf{GL}(n, \mathbb{C})$ is a group under matrix multiplication.

NOTE : The general linear group $\mathsf{GL}(n,\mathbb{C})$ is *connected*. This is in contrast with the fact that $\mathsf{GL}(n,\mathbb{R})$ has two components.

The complex special linear group $SL(n, \mathbb{C})$

This group is defined by

$$\mathsf{SL}(n,\mathbb{C}) := \{A \in \mathsf{GL}(n,\mathbb{C}) \,|\, \det A = 1\}$$

and is treated as in the real case. The matrix group $SL(n, \mathbb{C})$ is *not* compact but *connected*.

The unitary and special unitary groups U(n) and SU(n)

For $A = \begin{bmatrix} a_{ij} \end{bmatrix} \in \mathbb{C}^{n \times n}$,

$$A^* := \bar{A}^\top = A^\top$$

is the *Hermitian conjugate* (i.e., the conjugate transpose) matrix of A; thus, $(A^*)_{ij} = \bar{a}_{ji}$. The **unitary group** is defined as

$$\mathsf{U}(n) := \{ A \in \mathsf{GL}(n, \mathbb{C}) \, | \, A^*A = I_n \}.$$

♦ **Exercise 194** Verify that U(n) is a *subgroup* of the general linear group $GL(n, \mathbb{C})$.

The unitary condition amounts to n^2 equations for the n^2 complex numbers $a_{ij}, i, j = 1, 2, ..., n$

$$\sum_{k=1}^{n} \bar{a}_{ki} a_{kj} = \delta_{ij}.$$

By taking real and imaginary parts, these equations actually give $2n^2$ equations in the $2n^2$ real and imaginary parts of the a_{ij} (although there is some redundancy). This means that U(n) is a *closed* subset of $\mathbb{C}^{n \times n} = \mathbb{R}^{2n^2}$ and hence of $\mathsf{GL}(n,\mathbb{C})$. Thus U(n) is a complex matrix group.

NOTE : The unitary group U(n) is compact and connected.

Let $A \in U(n)$. From $|\det A| = 1$, we see that the determinant function $\det : \mathsf{GL}(n, \mathbb{C}) \to \mathbb{C}$ maps U(n) onto the unit circle $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}.$

NOTE : In the special case n = 1, a complex linear mapping $\phi : \mathbb{C} \to \mathbb{C}$ is multiplication by some complex number z, and ϕ is an *isometry* if and only if |z| = 1. In this way, the unitary group U(1) is *identified* with the unit circle \mathbb{S}^1 . The group U(1) is more commonly known as the *circle group* or the 1-dimensional *torus*, and is also denoted by \mathbb{T}^1 .

The dot product on \mathbb{R}^n can be extended to \mathbb{C}^n by setting (for $x, y \in \mathbb{C}^{n \times 1}$)

$$x \bullet y := x^* y = \bar{x}_1 y_1 + \bar{x}_2 y_2 + \dots + \bar{x}_n y_n.$$

NOTE : This is not \mathbb{C} -linear but satisfies (for $x, y \in \mathbb{C}^{n \times 1}$ and $u, v \in \mathbb{C}$)

$$(ux) \bullet (vy) = \bar{u}v(x \bullet y).$$

$$\|x\| := \sqrt{x \bullet x}.$$

Then a matrix $A \in \mathbb{C}^{n \times n}$ is unitary if and only if (for $x, y \in \mathbb{C}^n$)

$$Ax \bullet Ay = x \bullet y.$$

♦ **Exercise 195** If $G_i \leq \mathsf{GL}(n_i, \Bbbk)$, i = 1, 2 are matrix groups, show that their (direct) product $G_1 \times G_2$ is also a matrix group (in $\mathsf{GL}(n_1 + n_2, \Bbbk)$). Observe, in particular, that the k-dimensional torus

$$\mathbb{T}^k := \mathbb{T}^1 \times \mathbb{T}^1 \times \cdots \times \mathbb{T}^1$$

is a matrix group (in $\mathsf{GL}(k, \mathbb{C})$). These groups are compact connected Abelian matrix groups. In fact, they are the *only* matrix groups with these properties.

The special unitary group

$$SU(n) := \{A \in U(n) | \det A = 1\}$$

is a closed subgroup of U(n) and hence a complex matrix group.

NOTE : The matrix group SU(n) is *compact* and *connected*. In the special case n = 2, SU(2) is *diffeomorphic* to the unit sphere \mathbb{S}^3 in \mathbb{C}^2 (or \mathbb{R}^4). The group SU(2) is used in the construction of the gauge group for the Young-Mills equations in *elementary particle physics*. Also, there is a 2 to 1 surjection (in fact, a surjective submersion)

$$\pi:\mathsf{SU}\left(2\right)\to\mathsf{SO}\left(3\right)$$

which is of crucial importance in *computational mechanics* (it is related to the quaternionic representation of rotations in Euclidean 3-space).

The complex orthogonal groups $O(n, \mathbb{C})$ and $SO(n, \mathbb{C})$

Consider the bilinear form on (the vector space) \mathbb{C}^n defined by (for $x, y \in \mathbb{C}^n$)

$$(x, y) := x_1 y_1 + x_2 y_2 + \dots + x_n y_n.$$

This form is *not* an inner product because of the lack of complex conjugation in the definition. The set of all complex $n \times n$ matrices which preserve this form (i.e., such that (Ax, Ay) = (x, y) for all $x, y \in \mathbb{C}^n$) is the **complex** orthogonal group $O(n, \mathbb{C})$. Thus

$$\mathsf{O}(n,\mathbb{C}) := \left\{ A \in \mathsf{GL}(n,\mathbb{C}) \, | \, A^{\top}A = I_n \right\} \subseteq \mathsf{GL}(n,\mathbb{C}).$$

It is easy to show that $O(n,\mathbb{C})$ is a matrix group, and that det $A = \pm 1$ for all $O(n,\mathbb{C})$.

NOTE : The matrix group $O(n, \mathbb{C})$ is *not* the same as the unitary group U(n).

The complex special orthogonal group

$$\mathsf{SO}(n,\mathbb{C}) := \{A \in \mathsf{O}(n,\mathbb{C}) \mid \det A = 1\}$$

is also a matrix group.

The unipotent group $UT^{u}(n, \mathbb{k})$

A matrix $A = \begin{bmatrix} a_{ij} \end{bmatrix} \in \mathbb{k}^{n \times n}$ is upper triangular if all the entries below the main diagonal are equal to 0. Let $\mathsf{UT}(n,\mathbb{k})$ denote the set of all $n \times n$ invertible upper triangular matrices (over \mathbb{k}). Thus

$$\mathsf{UT}(n,\mathbb{k}) := \{ A \in \mathsf{GL}(n,\mathbb{k}) \,|\, a_{ij} = 0 \text{ for } i > j \}.$$

♦ **Exercise 196** Show that $UT(n, \Bbbk)$ is a *closed* subgroup of the general linear group $GL(n, \Bbbk)$ (and hence a matrix group).

The group $UT(n, \mathbb{k})$ is called the (real or complex) **upper triangular group**. This group is *not* compact.

NOTE : Likewise, one can define the *lower triangular group*

$$\mathsf{LT}(n, \Bbbk) := \{ A \in \mathsf{GL}(n, \Bbbk) \, | \, a_{ij} = 0 \text{ for } i < j \}$$

Clearly, $A \in \mathsf{LT}(n, \Bbbk)$ if and only if $A^{\top} \in \mathsf{UT}(n, \Bbbk)$. The matrix groups $\mathsf{UT}(n, \Bbbk)$ and $\mathsf{LT}(n, \Bbbk)$ are *isomorphic* and there is no need to distinguish between them.

♦ Exercise 197 Show that the diagonal group

$$\mathsf{D}(n,\Bbbk) := \{ A \in \mathsf{GL}(n,\Bbbk) \, | \, a_{ij} = 0 \text{ for } i \neq j \}$$

is a closed subgroup of $\mathsf{UT}(n, \Bbbk)$ (and hence a *matrix group*).

♦ **Exercise 198** For $k \leq n$, let $\mathsf{P}(k)$ denote the group of all linear transformations (i.e., invertible linear mappings) on \mathbb{R}^n that preserve the subspace $\mathbb{R}^k = \mathbb{R}^k \times \{0\} \subseteq \mathbb{R}^n$. Show that $\mathsf{P}(k)$ is (*isomorphic* to) the matrix group

$$\left\{ \begin{bmatrix} A & X \\ 0 & B \end{bmatrix} \mid A \in \mathsf{GL}(k, \mathbb{R}), B \in \mathsf{GL}(n-k, \mathbb{R}), X \in \mathbb{R}^{k \times (n-k)} \right\}$$

An upper triangular matrix $A = \begin{bmatrix} a_{ij} \end{bmatrix}$ is *unipotent* if it has all diagonal entries equal to 1. The (real or complex) **unipotent group** is (the subgroup of $\mathsf{GL}(n, \Bbbk)$)

$$\mathsf{UT}^{u}(n, \Bbbk) := \{A \in \mathsf{GL}(n, \Bbbk) \mid a_{ij} = 0 \text{ for } i > j \text{ and } a_{ii} = 1\}$$

(see also **Exercise 194**). It is easy to see that the unipotent group $UT^{u}(n, \mathbb{k})$ is a closed subgroup of $GL(n, \mathbb{k})$ and hence a *matrix group*.

NOTE : $\mathsf{UT}^{u}(n, \Bbbk)$ is a closed subgroup of $\mathsf{UT}(n, \Bbbk)$.

For the case

$$\mathsf{UT}^{u}\left(2,\mathbb{k}\right) = \left\{ \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \in \mathsf{GL}\left(n,\mathbb{k}\right) \, | \, t \in \mathbb{k} \right\}$$

the mapping

$$\boldsymbol{\theta}: \mathbb{k} \to \mathsf{UT}^u\left(2, \mathbb{k}\right), \quad t \mapsto \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$$

is a *continuous* group homomorphism which is an isomorphism with continuous inverse. This allows us to *view* \Bbbk *as a matrix group*.

NOTE : Given two matrix groups G and H, a group homomorphism $\theta: G \to H$ is a *continuous homomorphism* if it is continuous and its image $\theta(G) \leq H$ is a closed subset of H. For instance,

$$\theta: \mathsf{UT}^{u}(2,\mathbb{R}) \to \mathsf{U}(1), \quad \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \mapsto e^{2\pi t i}$$

is a continuous homomorphism of matrix groups, but (for $a \in \mathbb{R} \setminus \mathbb{Q}$)

$$\theta': G = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \in \mathsf{SUT}\left(2, \mathbb{R}\right) | k \in \mathbb{Z} \right\} \to \mathsf{U}\left(1\right), \quad \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \mapsto e^{2\pi kai}$$

is not (since its image is a dense proper subset of U(1)). Whenever we have a continuous homomorphism of matrix groups $\theta: G \to H$ which is a homeomorphism (i.e., a continuous bijection with continuous inverse) we say that θ is a continuous isomorphism and regard G and H as "identical" (as matrix groups).

The unipotent group $UT^{u}(3,\mathbb{R})$ is the **Heisenberg group**

$$\mathsf{Heis} := \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

which is particularly important in *quantum physics*; the *Lie algebra* of Heis gives a realization of the *Heisenberg commutation relations* of quantum mechanics.

 \diamond Exercise 199 Verify that the 4 \times 4 unipotent matrices A of the form

$$A = \begin{bmatrix} 1 & a_2 & a_3 & a_4 \\ 0 & 1 & a_1 & \frac{a_1^2}{2} \\ 0 & 0 & 1 & a_1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

form a closed subgroup of $\mathsf{UT}^u(4,\mathbb{R})$ (and hence a matrix group). Generalize.

Several other matrix groups are of great interest. We describe briefly some of them.

The general affine group GA(n, k)

The general affine group (over k) is the group

$$\mathsf{GA}\left(n,\Bbbk\right) := \left\{ \begin{bmatrix} 1 & 0 \\ c & A \end{bmatrix} \in \mathsf{GL}\left(n+1, \Bbbk\right) \, | \, c \in \Bbbk^{n \times 1} \ \text{ and } \ A \in \mathsf{GL}\left(n, \Bbbk\right) \right\}.$$

This is clearly a closed subgroup of the general linear group $\mathsf{GL}(n+1,\Bbbk)$ (and hence a *matrix group*). The general affine group $\mathsf{GA}(n,\Bbbk)$ is *not* compact. Likewise the case of the general linear group, the matrix group $\mathsf{GA}(n,\mathbb{C})$ is connected but $\mathsf{GA}(n,\mathbb{R})$ is *not*. NOTE : If we identify the element $x \in \mathbb{k}^n$ with $\begin{bmatrix} 1 \\ x \end{bmatrix} \in \mathbb{k}^{(n+1)\times 1}$, then since $\begin{bmatrix} 1 & 0 \\ c & A \end{bmatrix} \begin{bmatrix} 1 \\ x \end{bmatrix} = \begin{bmatrix} 1 \\ Ax + c \end{bmatrix}$

we obtain an *action* of the group $\mathsf{GA}(n, \Bbbk)$ on (the vector space) \Bbbk^n . Transformations on \Bbbk^n having the form $x \mapsto Ax + c$ (with A invertible) are called *affine transformations* and they preserve *lines* (i.e., translates of 1-dimensional subspaces of the vector space \Bbbk^n). The associated geometry is *affine geometry* that has $\mathsf{GA}(n, \Bbbk)$ as its symmetry group.

The (additive group of the) vector space \mathbb{k}^n (in fact, $\mathbb{k}^{n \times 1}$) can be viewed as (and identified with) the *translation subgroup* of $\mathsf{GA}(n,\mathbb{k})$

$$\left\{ \begin{bmatrix} 1 & 0 \\ c & I_n \end{bmatrix} \in \mathsf{GL}\left(n+1, \mathbb{k}\right) \, | \, c \in \mathbb{k}^{n \times 1} \right\} \le \mathsf{GA}\left(n, \mathbb{k}\right)$$

and this is a closed subgroup.

The identity component of the (real) general affine group $GA(n, \mathbb{R})$ is (the matrix group)

$$\mathsf{GA}^{+}(n,\mathbb{R}) = \left\{ \begin{bmatrix} 1 & 0 \\ c & A \end{bmatrix} \mid c \in \mathbb{k}^{n \times 1} \text{ and } A \in \mathsf{GL}^{+}(n,\mathbb{R}) \right\}.$$

In particular,

$$\mathsf{GA}^{+}(1,\mathbb{R}) = \left\{ \begin{bmatrix} 1 & 0 \\ c & e^{a} \end{bmatrix} \mid a,c \in \mathbb{R} \right\}$$

is a *connected* matrix group (of "dimension" 2). Its elements are (in fact, can be identified with) transformations on (the real line) \mathbb{R} having the form $x \mapsto bx + c$ (with $b, c \in \mathbb{R}$ and b > 0).

The Euclidean group $\mathsf{E}(n)$

This is the matrix group

$$\mathsf{E}(n) := \left\{ \begin{bmatrix} 1 & 0 \\ c & A \end{bmatrix} \in \mathsf{GL}(n+1,\mathbb{R}) \, | \, c \in \mathbb{R}^{n \times 1} \text{ and } A \in \mathsf{O}(n) \right\}.$$

The Euclidean group $\mathsf{E}(n)$ is a closed subgroup of the general affine group $\mathsf{GA}(n,\mathbb{R})$ and also is neither compact nor connected. It can be viewed as (and thus identified with) the group of all *isometries* (i.e., *rigid motions*) on the Euclidean n-space \mathbb{R}^n .

The special Euclidean group SE(n)

The special Euclidean group SE(n) is (the matrix group) defined by

$$\mathsf{SE}(n) := \left\{ \begin{bmatrix} 1 & 0 \\ c & R \end{bmatrix} \in \mathsf{GL}(n+1,\mathbb{R}) \, | \, c \in \mathbb{R}^{n \times 1} \text{ and } R \in \mathsf{SO}(n) \right\}.$$

This group is *isomorphic* to the group of all *orientation-preserving isometries* (i.e., *proper rigid motions*) on the Euclidean n-space \mathbb{R}^n . It is *not* compact but *connected*.

Some other groups

Several important groups which are not naturally groups of matrices can be viewed as matrix groups. We have seen that the multiplicative groups \mathbb{R}^{\times} and \mathbb{C}^{\times} (of non-zero real numbers and complex numbers, respectively) are *isomorphic* to the matrix groups $\mathsf{GL}(1,\mathbb{R})$ and $\mathsf{GL}(1,\mathbb{C})$, respectively. Also, the *circle group* \mathbb{S}^1 (of complex numbers with absolute value one) is *isomorphic* to $\mathsf{U}(1)$. The *n*-torus (the direct product of *n* copies of \mathbb{S}^1)

$$\mathbb{T}^n = \mathbb{S}^1 \times \cdots \times \mathbb{S}^1 \leq \mathsf{GL}\left(n, \mathbb{C}\right)$$

is *isomorphic* to the matrix group of $n \times n$ diagonal matrices with complex entries of modulus one. (\mathbb{T}^n can also be realized as the *quotient group* $\mathbb{R}^n/\mathbb{Z}^n$: an element $(\theta_1, \ldots, \theta_n) \mod \mathbb{Z}^n$ of $\mathbb{R}^n/\mathbb{Z}^n$ can be identified with the diagonal matrix diag $(e^{2\pi i \theta_1}, \ldots, e^{2\pi i \theta_n})$.)

NOTE : If $\theta : G \to H$ is a continuous homomorphism of matrix groups, then its *kernel* ker $\theta \leq G$ is a matrix group. Moreover, the *quotient group* $G/\ker \theta$ can be identified with the matrix group $\theta(G)$ by the usual quotient isomorphism $\tilde{\theta}$: $G/\ker \theta \to \theta(G)$.

However, it is important to realize that not every normal matrix subgroup N of the matrix group G gives rise to a matrix group G/N; there are examples for which G/N is a *Lie group* but not a matrix group. (We shall see later that every matrix group is a Lie group.)

Recall that the additive groups \mathbb{R} and \mathbb{C} are *isomorphic* to the unipotent groups $\mathsf{UT}^{u}(2,\mathbb{R})$ and $\mathsf{UT}^{u}(2,\mathbb{C})$, respectively.

\diamond **Exercise 200** Verify that the map

$$x \in \mathbb{R} \mapsto [e^x] \in \mathsf{GL}^+(1,\mathbb{R})$$

is a *continuous isomorphism* of matrix groups, and then show that the additive group \mathbb{R}^n is *isomorphic* to the matrix group of all $n \times n$ diagonal matrices with positive entries.

 \diamond **Exercise 201** Let $\mathbb{Z}^n \leq \mathbb{R}^n$ be the *discrete* subgroup of vectors with integer entries and set

$$\mathsf{GL}(n,\mathbb{Z}) := \{A \in \mathsf{GL}(n,\mathbb{R}) \,|\, A(\mathbb{Z}^n) = \mathbb{Z}^n\}.$$

Show that $\mathsf{GL}(n,\mathbb{Z})$ is a matrix group. (This matrix group consists of $n \times n$ matrices over (the ring) \mathbb{Z} with determinant ± 1 .)

The symmetric group S_n of all permutations on n elements may be considered as well as a matrix group. Indeed, we can make S_n to act (from the right) on \mathbb{k}^n by linear transformations :

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \cdot \sigma = \begin{bmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{bmatrix}.$$

Thus (for the standard unit vectors e_1, e_2, \ldots, e_n) $e_i \cdot \sigma = e_{\sigma(i)}, \quad i = 1, 2, \ldots, n.$

The matrix $[\sigma]$ of the linear transformation induced by $\sigma \in S_n$ (with respect to the standard basis) has all its entries 0 or 1, with exactly one 1 in each row and column. Such a matrix is usually called a *permutation matrix*.

♦ **Exercise 202** Write down the permutations matrices induces by the elements (permutations) of S_3 .

When $\mathbb{k} = \mathbb{R}$ each of these permutation matrices is orthogonal, while when $\mathbb{k} = \mathbb{C}$ it is unitary. So, for a given $n \ge 1$, the symmetric group S_n is (isomorphic to) a closed subgroup of $\mathsf{O}(n)$ or $\mathsf{U}(n)$.

NOTE : Any *finite* group is (isomorphic to) a matrix subgroup of some orthogonal group O(n).

The following table lists some interesting matrix groups, indicates whether or not the group is compact and/or connected, and gives the number of (connected) components.

Group	Compact ?	Connected ?	Components
$GL\left(n,\mathbb{C} ight)$	no	yes	one
$SL\left(n,\mathbb{C} ight)$	no	yes	one
$GL\left(n,\mathbb{R} ight)$	no	no	two
$GL^{+}\left(n,\mathbb{R}\right)$	no	yes	one
$SL\left(n,\mathbb{R} ight)$	no	yes	one
$U\left(n ight)$	yes	yes	one
$SU\left(n ight)$	yes	yes	one
$O\left(n ight)$	yes	no	two
$SO\left(n ight)$	yes	yes	one
$O\left(1,n ight)$	no	no	four
$SO\left(1,n ight)$	no	no	two
Lor(1,n)	no	yes	one
$Sp\left(2n,\mathbb{R} ight)$	no	yes	one
$UT^{u}\left(n,\Bbbk ight)$	no	yes	one
$GA\left(n,\Bbbk\right)$	no	no	two
$GA^{+}\left(n,\Bbbk\right)$	no	yes	one
$E\left(n ight)$	no	no	two
$SE\left(n ight)$	no	yes	one
\mathbb{R}^{n}	no	yes	one
\mathbb{T}^n	yes	yes	one

NOTE : There are more interesting matrix groups, e.g., the *quaternionic matrix* groups (in particular, the quaternionic symplectic group Sp(n)), associated with the

division algebra \mathbb{H} of quaternions, as well as the *spinor groups* $\mathsf{Spin}(n)$ and the *pinor groups* $\mathsf{Pin}(n)$, associated with (real) Clifford algebras.

Complex matrix groups as real matrix groups

Recall that the (complex) vector space \mathbb{C} can be viewed as a *real* 2-dimensional vector space (with basis $\{1, i\}$, for example).

♦ Exercise 203 Show that the mapping

$$\rho : \mathbb{C} \to \mathbb{R}^{2 \times 2}, \quad z = x + iy \mapsto \begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

is an injective ring homomorphism (i.e., a one-to-one mapping such that, for $z, z' \in \mathbb{C}$,

$$\rho(z+z')=\rho(z)+\rho(z') \quad \text{and} \quad \rho(zz')=\rho(z)\rho(z').)$$

We can view \mathbb{C} as a *subring* of $\mathbb{R}^{2\times 2}$. In other words, we can *identify* the complex number z = x + iy with the 2×2 real matrix $\rho(z)$.

NOTE : This can also be expressed as

$$\rho(x+iy) = xI_2 - yJ_2, \quad \text{where} \quad J_2 := \begin{bmatrix} 0 & 1\\ -1 & 0 \end{bmatrix}.$$

Also, for $z \in \mathbb{C}$,

$$\rho(\bar{z}) = \rho(z)^T$$

(complex conjugation corresponds to transposition).

More generally, given $Z = [z_{rs}] \in \mathbb{C}^{n \times n}$ with $z_{rs} = x_{rs} + iy_{rs}$, we can write

$$Z = X + iY,$$

where $X = \begin{bmatrix} x_{rs} \end{bmatrix}$, $Y = \begin{bmatrix} y_{rs} \end{bmatrix} \in \mathbb{R}^{n \times n}$.

 $\diamond~Exercise~204~$ Show that the mapping

$$\rho_n : \mathbb{C}^{n \times n} \to \mathbb{R}^{2n \times 2n}, \quad Z = X + iY \mapsto \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix}$$

is an injective ring homomorphism.

Hence we can *identify* the complex matrix Z = X + iY with the $2n \times 2n$ real matrix $\rho_n(Z)$. Let

$$\mathbb{J} = \mathbb{J}_{2n} := \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \in \mathsf{SL}(2n, \mathbb{R}).$$

Then we can write

$$\rho_n(Z) = \rho_n(X + iY) = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} - \begin{bmatrix} Y & 0 \\ 0 & Y \end{bmatrix} \mathbb{J}.$$

 $\diamond~Exercise~205~$ First verify that

$$\mathbb{J}^2 = -I_{2n}$$
 and $\mathbb{J}^\top = -\mathbb{J}$

and then show that, for $Z \in \mathbb{C}^{n \times n}$,

$$\rho_n(\bar{Z}) = \rho_n(Z)^\top \iff X = X^\top \text{ and } Y = Y^\top.$$

We see that $\rho_n(\mathsf{GL}(n,\mathbb{C}))$ is a closed subgroup of $\mathsf{GL}(2n,\mathbb{R})$, so any matrix subgroup G of $\mathsf{GL}(n,\mathbb{C})$ can be viewed as a matrix subgroup of $\mathsf{GL}(2n,\mathbb{R})$ (by identifying it with its image $\rho_n(G)$ under ρ_n). The following characterizations are sometimes useful :

$$\begin{split} \rho_n(\mathbb{C}^{n \times n}) &= & \left\{ A \in \mathbb{R}^{n \times n} \, | \, A \mathbb{J} = \mathbb{J}A \right\} \\ \rho_n(\mathsf{GL}\left(n, \mathbb{C}\right)) &= & \left\{ A \in \mathsf{GL}\left(2n, \mathbb{R}\right) \, | \, A \mathbb{J} = \mathbb{J}A \right\}. \end{split}$$

 \diamond **Exercise 206** Verify the following set of equalities :

$$\begin{split} \rho_n(\mathsf{U}\,(n)) &= &\mathsf{O}\,(n) \cap \rho_n(\mathsf{GL}\,(n,\mathbb{C})) \\ &= &\mathsf{O}\,(n) \cap \mathsf{Sp}\,(2n,\mathbb{R}) \\ &= &\rho_n(\mathsf{GL}\,(n,\mathbb{C})) \cap \mathsf{Sp}\,(2n,\mathbb{R}). \end{split}$$

NOTE: In a slight abuse of notation, the real symplectic group $\mathsf{Sp}(2n, \mathbb{R})$ is related to the unitary group $\mathsf{U}(n)$ by

$$\mathsf{Sp}(2n,\mathbb{R})\cap\mathsf{O}(2n)=\mathsf{U}(n).$$

4.3 The Exponential Mapping

Let $A \in \mathbb{k}^{n \times n}$ and consider the matrix series

$$\sum_{k \ge 0} \frac{1}{k!} A^k = I_n + A + \frac{1}{2!} A^2 + \frac{1}{3!} A^3 + \cdots$$

NOTE : This matrix series is a series in the complete normed vector space (in fact, algebra) $(\mathbb{k}^{n \times n}, \|\cdot\|)$, where $\|\cdot\|$ is the *operator norm* (induced by the Euclidean norm on \mathbb{k}^n). In a complete normed vector space, an absolutely convergent series $\sum_{k\geq 0} a_k$ (i.e., such that the series $\sum_{k\geq 0} \|a_k\|$ is convergent) is convergent, and

$$\left\|\sum_{k=0}^{\infty} a_k\right\| \le \sum_{k=0}^{\infty} \|a_k\|.$$

(The converse is not true.) Also, every *rearrangement* of an absolutely convergent series is absolutely convergent, with same sum. Given two absolutely convergent series $\sum_{k\geq 0} a_k \text{ and } \sum_{k\geq 0} b_k \text{ (in a complete normed algebra), their Cauchy product } \sum_{k\geq 0} c_k, \text{ where}$ $c_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 \text{ is also absolutely convergent, and}$ $\sum_{i+j=k}^{\infty} c_k = \left(\sum_{k=0}^{\infty} a_k\right) \left(\sum_{k=0}^{\infty} b_k\right)$

$$\sum_{k=0}^{\infty} c_k = \left(\sum_{k=0}^{\infty} a_k\right) \left(\sum_{k=0}^{\infty} b_k\right).$$

♦ **Exercise 207** Show that the matrix series $\sum_{k\geq 0} \frac{1}{k!} A^k$ is absolutely convergent (and hence convergent).

Let $\sum_{k=0}^{\infty} \frac{1}{k!} A^k$ denote the *sum* of the (absolutely) convergent matrix series $\sum_{k\geq 0} \frac{1}{k!} A^k$. We set

$$e^{A} = \exp(A) := \sum_{k=0}^{\infty} \frac{1}{k!} A^{k}.$$

This matrix is called the **matrix exponential** of A. It follows that

$$\|\exp(A)\| \le \|I_n\| + \|A\| + \frac{1}{2!}\|A\|^2 + \dots = e^{\|A\|}$$

and also $\|\exp(A) - I_n\| \le e^{\|A\|} - 1.$

♦ **Exercise 208** Show that (for $\lambda, \mu \in \mathbb{k}$)

$$\exp\left((\lambda + \mu)A\right) = \exp\left(\lambda A\right)\exp\left(\mu A\right).$$

[HINT : These series are absolutely convergent. Think of the Cauchy product.]

It follows that

$$I_n = \exp(O) = \exp((1 + (-1))A) = \exp(A)\exp(-A)$$

and hence $\exp(A)$ is *invertible* with inverse $\exp(-A)$. So $\exp(A) \in \mathsf{GL}(n, \Bbbk)$.

NOTE: The "group property" $\exp((\lambda + \mu)A) = \exp(\lambda A) \exp(\mu A)$ may be rephrased by saying that, for fixed $A \in \mathbb{k}^{n \times n}$, the mapping $\lambda \mapsto \exp(\lambda A)$ is a (continuous) *homomorphism* from the additive group of scalars \mathbb{k} into the general linear group $\mathsf{GL}(n,\mathbb{k})$.

4.3.1 DEFINITION. The mapping

$$\exp: \mathbb{k}^{n \times n} \to \mathsf{GL}\left(n, \mathbb{k}\right), \quad A \mapsto \exp\left(A\right)$$

is called the **exponential mapping**.

4.3.2 PROPOSITION. If $A, B \in \mathbb{k}^{n \times n}$ commute, then

$$\exp\left(A+B\right) = \exp\left(A\right)\exp\left(B\right).$$

PROOF: We expand the series and perform a sequence of manipulations that

are legitimate since these series are absolutely convergent :

$$\exp(A) \exp(B) = \left(\sum_{r=0}^{\infty} \frac{1}{r!} A^r\right) \left(\sum_{s=0}^{\infty} \frac{1}{s!} B^s\right)$$
$$= \sum_{r,s=0}^{\infty} \frac{1}{r!s!} A^r B^s$$
$$= \sum_{k=0}^{\infty} \left(\sum_{r=0}^k \frac{1}{r!(k-r)!} A^r B^{k-r}\right)$$
$$= \sum_{k=0}^{\infty} \frac{1}{k!} \left(\sum_{r=0}^k \binom{k}{r} A^r B^{k-r}\right)$$
$$= \sum_{k=0}^{\infty} \frac{1}{k!} (A+B)^k$$
$$= \exp(A+B).$$

-		

NOTE: We have made crucial use of the *commutativity* of A and B in the identity

$$\sum_{r=0}^k \binom{k}{r} A^r B^{k-r} = (A+B)^k.$$

In particular, for the (commuting) matrices λA and μA , we reobtain the property $\exp((\lambda + \mu)A) = \exp(\lambda A)\exp(\mu A)$. It is important to realize that, in fact, the following statements are equivalent (for $A, B \in \mathbb{k}^{n \times n}$):

- (i) AB = BA.
- (ii) $\exp(\lambda A) \exp(\mu B) = \exp(\mu B) \exp(\lambda A)$ for all $\lambda, \mu \in \mathbb{k}$.
- (iii) $\exp(\lambda A + \mu B) = \exp(\lambda A) \exp(\mu B)$ for all $\lambda, \mu \in \mathbb{k}$.

♦ **Exercise 209** Compute (for $a, b \in \mathbb{R}$)

$$\exp\left(\begin{bmatrix}a & 0\\ 0 & a\end{bmatrix}\right), \quad \exp\left(\begin{bmatrix}a & -b\\ b & a\end{bmatrix}\right), \quad \exp\left(\begin{bmatrix}a & b\\ b & a\end{bmatrix}\right), \quad \exp\left(\begin{bmatrix}a & b\\ 0 & a\end{bmatrix}\right).$$

NOTE : Every real 2×2 matrix is *conjugate* to exactly one of the following types (with $a, b \in \mathbb{R}, b \neq 0$):

•
$$a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
 (scalar).
• $a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ (elliptic).
• $a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (hyperbolic)
• $a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (parabolic).

Hermitian and skew-Hermitian matrices.

♦ Exercise 210

- (a) Show that if $A \in \mathbb{R}^{n \times n}$ is *skew-symmetric*, then $\exp(A)$ is orthogonal.
- (b) Show that if $A \in \mathbb{C}^{n \times n}$ is *skew-Hermitian*, then $\exp(A)$ is unitary.
- ♦ **Exercise 211** Let $A \in \mathbb{k}^{n \times n}$ and $B \in \mathsf{GL}(n, \mathbb{k})$. Show that

$$\exp(BAB^{-1}) = B \exp(A) B^{-1}.$$

Deduce that if $B^{-1}AB = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$, then

$$\exp(A) = B \operatorname{diag} \left(e^{\lambda_1}, e^{\lambda_2}, \dots, e^{\lambda_n} \right) B^{-1}.$$

♦ **Exercise 212** A matrix $A \in \mathbb{k}^{n \times n}$ is **nilpotent** if $A^k = O$ for some $k \ge 1$.

- (a) Prove that a nilpotent matrix is singular.
- (b) Prove that a strictly upper triangular matrix $A = \begin{bmatrix} a_{ij} \end{bmatrix}$ (i.e. with $a_{ij} = 0$ whenever $i \ge j$) is nilpotent.
- (c) Find two nilpotent matrices whose product is *not* nilpotent.

 \diamond **Exercise 213** Suppose that $A \in \mathbb{k}^{n \times n}$ and ||A|| < 1.

(a) Show that the matrix series

$$\sum_{k\geq 0} A^k = I_n + A + A^2 + A^3 + \cdots$$

converges (in $\mathbb{k}^{n \times n}$).

(b) Show that the matrix $I_n - A$ is *invertible* and find a formula for $(I_n - A)^{-1}$.

(c) If A is *nilpotent*, determine $(I_n - A)^{-1}$ and $\exp(A)$.

♦ **Exercise 214** Show (for $\lambda \in \mathbb{R}$)

$$\exp\left(\begin{bmatrix}\lambda & 1 & 0 & \dots & 0\\ 0 & \lambda & 1 & \dots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \dots & \lambda\end{bmatrix}\right) = \begin{bmatrix}e^{\lambda} & e^{\lambda} & \frac{1}{2!}e^{\lambda} & \dots & \frac{1}{(n-1)!}e^{\lambda}\\ 0 & e^{\lambda} & e^{\lambda} & \dots & \frac{1}{(n-2)!}e^{\lambda}\\ \vdots & \vdots & \vdots & & \vdots\\ 0 & 0 & 0 & \dots & e^{\lambda}\end{bmatrix}$$

NOTE : When the matrix $A \in \mathbb{k}^{n \times n}$ is *diagonalizable* over \mathbb{C} (i.e., $A = C \operatorname{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) C^{-1}$ for some $C \in \mathsf{GL}(n, \mathbb{C})$), we have

$$\exp(A) = C \operatorname{diag} \left(e^{\lambda_1}, e^{\lambda_2}, \dots, e^{\lambda_n} \right) C^{-1}.$$

This means that the problem of calculating the exponential of a diagonalizable matrix is solved once an explicit diagonalization is found. Many important types of matrices are indeed diagonalizable (over \mathbb{C}), including skew-symmetric, skew-Hermitian, orthogonal, and unitary matrices. However, there are also many non-diagonalizable matrices. If $A^k = O$ for some positive integer k, then $A^{\ell} = O$ for all $\ell \geq k$. In this case the matrix series which defines $\exp(A)$ terminates after the first k terms, and so can be computed explicitly. A general matrix A may be neither nilpotent nor diagonalizable. This situation is best discussed in terms of the *Jordan canonical* form.

For $\lambda \in \mathbb{C}$ and $r \geq 1$, we have the Jordan block matrix

$$J(\lambda, r) := \begin{bmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{bmatrix} \in \mathbb{C}^{r \times r}.$$

The characteristic polynomial of $J(\lambda, r)$ is

$$\operatorname{char}_{J(\lambda,r)}(s) := \det \left(sI_r - J(\lambda,r) \right) = (s-\lambda)^r$$

and by the Cayley-Hamilton Theorem, $(J(\lambda, r) - \lambda I_r)^r = O$, which implies that $(J(\lambda, r) - \lambda I_r)^{r-1} \neq O$ (and hence $\operatorname{char}_{J(\lambda, r)}(s) = \min_{J(\lambda, r)}(s) \in \mathbb{C}[s]$). The main result on Jordan form is the following : Given $A \in \mathbb{C}^{n \times n}$, there exists a matrix

 $P \in \mathsf{GL}(n, \mathbb{C})$ such that

$$P^{-1}AP = \begin{bmatrix} J(\lambda_1, r_1) & O & \dots & O \\ O & J(\lambda_2, r_2) & \dots & O \\ \vdots & \vdots & & \vdots \\ O & O & \dots & J(\lambda_m, r_m) \end{bmatrix} \in \mathbb{C}^{n \times n}.$$

This form is unique except for the order in which the Jordan blocks $J(\lambda_i, r_i) \in \mathbb{C}^{r_i \times r_i}$ occur. (The elements $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the eigenvalues of A and in fact $\operatorname{char}_A(s) = (s - \lambda_1)^{r_1} (s - \lambda_2)^{r_2} \cdots (s - \lambda_m)^{r_m}$.)

Using the Jordan canonical form we can see that every matrix $A \in \mathbb{C}^{n \times n}$ can be written as A = S + N, where S is diagonalizable (over \mathbb{C}), N is nilpotent, and SN = NS.

$\diamond \text{ Exercise 215 Let } A \in \mathbb{k}^{n \times n}.$

- (a) Prove that A is *nilpotent* if and only if all its eigenvalues are equal to zero.
- (b) The matrix A is called **unipotent** if $I_n A$ is nilpotent (i.e. $(I_n A)^k = O$ for some $k \ge 1$). Prove that A is *unipotent* if and only if all its eigenvalues are equal to 1.
- (c) If A is a strictly upper triangular matrix, show that $\exp(A)$ is unipotent.

♦ Exercise 216 Compute

$$\exp\left(\begin{bmatrix}\lambda & a & b\\ 0 & \lambda & c\\ 0 & 0 & \lambda\end{bmatrix}\right).$$

♦ Exercise 217 The power series

$$\sum_{k\geq 1} (-1)^{k+1} \frac{(z-1)^k}{k} = z - 1 - \frac{(z-1)^2}{2} + \frac{(z-1)^3}{3} - \frac{(z-1)^4}{4} + \cdots, \quad z \in \mathbb{C}$$

has radius of convergence 1 and hence defines a complex analytic function

$$z \mapsto \log z := \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(z-1)^k}{k}$$

on the set $\{z \mid |z-1| < 1\}$. (This function coincides with the usual logarithm for real z on the interval (0, 2).) Show that
(a) For all z with |z - 1| < 1,

$$e^{\log z} = z.$$

(b) For all w with $|w| < \ln 2$, $|e^w - 1| < 1$ and

$$\log\left(e^{w}\right) = w.$$

Let $A \in \mathbb{k}^{n \times n}$. The matrix series

$$\sum_{k\geq 1} \frac{(-1)^{k+1}}{k} A^k = A - \frac{1}{2}A + \frac{1}{3}A^3 - \frac{1}{4}A^4 + \cdots$$

converges (absolutely) for ||A|| < 1. We define the logarithm mapping

$$\log : \mathcal{B}_{\mathbb{k}^{n \times n}}(I_n, 1) \to \mathbb{k}^{n \times n}, \quad A \mapsto \log \left(A\right) := \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} (A - I_n)^k.$$

(The notation $\mathcal{B}_{\mathbb{k}^{n\times n}}(A,\rho)$ stands for the *open ball* of radius ρ around A in the metric space $\mathbb{k}^{n\times n}$; that is,

$$\mathcal{B}_{\mathbb{k}^{n \times n}}(A, \rho) := \left\{ A' \in \mathbb{k}^{n \times n} \, | \, \|A' - A\| < \rho \right\}.)$$

NOTE : Defining a logarithm for matrices turns out to be at least as difficult as defining a logarithm for complex numbers, and so we cannot hope to define the matrix logarithm for all matrices, or even for all invertible matrices. We content ourselves with defining the logarithm in a *neighborhood* of the identity matrix. The logarithm mapping is *continuous* (on the set of all $n \times n$ matrices A with $||A - I_n|| < 1$) and $\log(A)$ is real if A is real.

 \diamond Exercise 218 Show that

(a) For all A with $||A - I_n|| < 1$,

$$\exp\left(\log\left(A\right)\right) = A.$$

(b) For all B with $\|B\| < \ln 2, \ \|\exp\left(B\right) - I_n\| < 1$ and

$$\log\left(\exp\left(B\right)\right) = B.$$

The exponential and logarithm mappings

 $\exp: \mathbb{k}^{n \times n} \to \mathsf{GL}\left(n, \mathbb{k}\right), \quad \text{and} \quad \log: \mathcal{B}_{\mathbb{k}^{n \times n}}(I_n, 1) \to \mathbb{k}^{n \times n}$

are continuous (in fact, infinitely differentiable). Indeed, since any power A^k is a continuous mapping of A, the sequence of partial sums $\left(\sum_{k=0}^r \frac{1}{k!}A^k\right)_{r\geq 0}$ consists of continuous mappings. But (it is easy to see that) the matrix series (defining the exponential matrix) converges uniformly on each set of the form $\{A \mid ||A|| \leq \rho\}$, and so the sum (i.e., the limit of its sequence of partial sums) is again continuous. (A similar argument works in the case of the logarithm mapping.)

By continuity (of the exponential mapping at the origin O), there is a number $\delta > 0$ such that

$$\mathcal{B}_{\mathbb{k}^{n\times n}}(O,\delta) \subseteq \exp^{-1}\left(\mathcal{B}_{\mathsf{GL}(n,\mathbb{k})}(I_n,1)\right).$$

In fact we can actually take $\delta = \ln 2$ since

$$\exp\left(\mathcal{B}_{\mathbb{k}^{n\times n}}(O,\delta)\right)\subseteq \mathcal{B}_{\mathbb{k}^{n\times n}}\left(I_n,e^{\delta}-1\right).$$

Hence we have the following result

4.3.3 PROPOSITION. The exponential mapping exp is injective when restricted to the open subset $\mathcal{B}_{\mathbb{k}^{n\times n}}(O, \ln 2)$. (Hence it is locally a diffeomorphism at the origin O with local inverse log.)

Let $A \in \mathbb{k}^{n \times n}$. For every $t \in \mathbb{R}$, the matrix series $\sum_{k \ge 0} \frac{t^k}{k!} A^k$ is (absolutely)

convergent and we have

$$\sum_{k=0}^{\infty} \frac{t^k}{k!} A^k = \sum_{k=0}^{\infty} \frac{1}{k!} (tA)^k = \exp(tA).$$

So the mapping

$$\alpha: \mathbb{R} \to \mathbb{k}^{n \times n}, \quad t \mapsto \exp(tA)$$

is defined and *differentiable* with

$$\dot{\alpha}(t) = \sum_{k=1}^{\infty} \frac{t^{k-1}}{(k-1)!} A^k = \exp{(tA)} A = A \exp{(tA)}.$$

NOTE : This mapping can be viewed as a *curve* in $\mathbb{k}^{n \times n}$. The curve is in fact *smooth* (i.e., infinitely differentiable) and satisfies the differential equation (in matrices) $\dot{\alpha}(t) = \alpha(t)A$ with initial condition $\alpha(0) = I_n$. Also (for $t, s \in \mathbb{R}$),

$$\alpha(t+s) = \alpha(t)\alpha(s).$$

In particular, this shows that $\alpha(t)$ is always invertible with $\alpha(t)^{-1} = \alpha(-t)$.

♦ **Exercise 219** Let $A, C \in \mathbb{k}^{n \times n}$. Show that the differential equation (in matrices) $\dot{\alpha} = \alpha A$ has a *unique* differentiable solution $\alpha : \mathbb{R} \to \mathbb{k}^{n \times n}$ for which $\alpha(0) = C$. (This solution is $\alpha(t) = C \exp(tA)$.) Furthermore, if C is invertible, then so is $\alpha(t)$ for $t \in \mathbb{R}$, hence $\alpha : \mathbb{R} \to \mathsf{GL}(n, \mathbb{k})$.

♦ **Exercise 220** Let $A \in \mathbb{k}^{n \times n}$. Show that the functional equation (in matrices) $\alpha(t+s) = \alpha(t)\alpha(s)$ has a *unique* differentiable solution $\alpha : \mathbb{R} \to \mathbb{k}^{n \times n}$ for which $\alpha(0) = I_n$ and $\dot{\alpha}(0) = A$. (This solution is $\alpha(t) = \exp(tA)$.)

♦ **Exercise 221** If $A, B \in \mathbb{k}^{n \times n}$ commute, show that

$$\left. \frac{d}{dt} \exp\left(A + tB\right) \right|_{t=0} = \exp\left(A\right)B = B \exp\left(A\right).$$

(This is a formula for the *derivative* of the exponential mapping exp at an arbitrary A, evaluated only at those B such that AB = BA. The general situation is more complicated.)

4.4 Lie Algebras for Matrix Groups

One-parameter subgroups

Let $G \leq \mathsf{GL}(n, \Bbbk)$ be a matrix group and let I denote the identity matrix.

NOTE : The matrix I is the *neutral element* of the group G. When $\mathbb{k} = \mathbb{R}$, then $I = I_n$ whereas when $\mathbb{k} = \mathbb{C}$ and $G \leq \mathsf{GL}(2n, \mathbb{R})$, then $I = I_{2n} = \begin{bmatrix} I_n & 0 \\ 0 & I_n \end{bmatrix}$.

4.4.1 DEFINITION. A **one-parameter subgroup** of G is a continuous mapping

$$\gamma: \mathbb{R} \to G$$

which is *differentiable* at 0 and satisfies (for $t, s \in \mathbb{R}$)

$$\gamma(s+t) = \gamma(s)\gamma(t)$$

We refer to the last condition as the homomorphism property.

NOTE : Recall that \mathbb{R} and G can be viewed as matrix groups (isomorphic to $UT^{u}(2,\mathbb{R})$ and to a subgroup of either $GL(n,\mathbb{R})$ or $GL(2n,\mathbb{R})$, respectively). Hence, γ is a *continuous homomorphism* of matrix groups.

It suffices to know γ on some open neighborhood $(-\varepsilon, \varepsilon)$ of 0 in \mathbb{R} . Indeed, let $t \in \mathbb{R}$. Then for some (large enough) natural number $m, \frac{t}{m} \in (-\varepsilon, \varepsilon)$. Hence

$$\gamma\left(\frac{t}{m}\right), \ \left(\gamma\left(\frac{t}{m}\right)\right)^m \in G.$$

♦ **Exercise 222** Show that (for $m, n \in \mathbb{N}$ such that $\frac{t}{m}, \frac{t}{n} \in (-\varepsilon, \varepsilon)$)

$$\left(\gamma\left(\frac{t}{n}\right)\right)^n = \left(\gamma\left(\frac{t}{m}\right)\right)^m$$

The element $\left(\gamma\left(\frac{t}{m}\right)\right)^m \in G$ is well defined (for every $t \in \mathbb{R}$), and so

$$\gamma(t) = \gamma\left(\frac{t}{m} + \frac{t}{m} + \dots + \frac{t}{m}\right) = \left(\gamma\left(\frac{t}{m}\right)\right)^m$$

NOTE : A one-parameter subgroup $\gamma : \mathbb{R} \to G$ can be viewed as a *collection* $(\gamma(t))_{t \in \mathbb{R}}$ of linear transformations on \mathbb{k}^n such that (for $t, s \in \mathbb{R}$)

- $\bullet \quad \gamma(0)=id_{\,\Bbbk^n}\,(=I).$
- $\gamma(s+t) = \gamma(s)\gamma(t).$
- $\gamma(t) \in G$ depends continuously on t.

Moreover, the curve $\gamma : \mathbb{R} \to G$ in $G \subseteq \mathbb{k}^{n \times n}$ has a tangent vector $\dot{\gamma}(0)$ (at $\gamma(0) = I$).

4.4.2 PROPOSITION. Let $\gamma : \mathbb{R} \to G$ be a one-parameter subgroup of G. Then γ is differentiable at every $t \in \mathbb{R}$ and

$$\dot{\gamma}(t) = \dot{\gamma}(0)\gamma(t) = \gamma(t)\dot{\gamma}(0).$$

PROOF : We have (for $t, h \in \mathbb{R}$)

$$\dot{\gamma}(t) = \lim_{h \to 0} \frac{1}{h} \left(\gamma(t+h) - \gamma(t) \right)$$
$$= \lim_{h \to 0} \frac{1}{h} \left(\gamma(h)\gamma(t) - \gamma(t) \right)$$
$$= \left(\lim_{h \to 0} \frac{1}{h} \left(\gamma(h) - I \right) \right) \gamma(t)$$
$$= \dot{\gamma}(0)\gamma(t)$$

and similarly

$$\dot{\gamma}(t) = \gamma(t)\dot{\gamma}(0).$$

We can now determine the form of all one-parameter subgroups of G.

4.4.3 THEOREM. Let $\gamma : \mathbb{R} \to G$ be a one-parameter subgroup of G. Then it has the form

$$\gamma(t) = \exp(tA)$$

for some $A \in \mathbb{k}^{n \times n}$.

PROOF: Let $A = \dot{\gamma}(0)$. This means that γ satisfies (the differential equation)

$$\dot{\gamma}(t) = A\gamma(t)$$

and is subject to (the initial condition)

$$\gamma(0) = I.$$

This initial value problem (IVP) has the unique solution $\gamma(t) = \exp(tA)$. \Box

We cannot yet reverse this process and decide for which $A \in \mathbb{k}^{n \times n}$ the one-parameter subgroup

$$\gamma : \mathbb{R} \to \mathsf{GL}(n, \mathbb{k}), \quad t \mapsto \exp(tA)$$

actually takes values in G. The answer involves the Lie algebra of G.

NOTE : We have a curious phenomenon in the fact that although the definition of a one-parameter group only involves first order differentiability, the general form $\exp(tA)$ is always infinitely differentiable (and indeed *analytic*) as a function of t. This is an important characteristic of much of the *Lie theory*, namely that conditions of first order differentiability (and even continuity) often lead to much stronger conditions.

Lie algebras

Let $G \leq \mathsf{GL}(n, \mathbb{k})$ be a matrix group. Recall that $\mathbb{k}^{n \times n}$ may be considered to be some Euclidean space \mathbb{R}^m .

4.4.4 DEFINITION. A curve in G is a *differentiable* mapping

$$\gamma:(a,b)\subseteq\mathbb{R}\to\Bbbk^{n\times n}$$

such that (for $t \in (a, b)$)

$$\gamma(t) \in G.$$

The derivative

$$\dot{\gamma}(t) := \lim_{h \to 0} \frac{1}{h} \left(\gamma(t+h) - \gamma(t) \right) \in \mathbb{k}^{n \times n}$$

is called the **tangent vector** to γ at $\gamma(t)$. We will usually assume that a < 0 < b.

♦ **Exercise 223** Given two curves $\gamma, \sigma : (a, b) \rightarrow G$, we define a new curve, the *product curve*, by

$$(\gamma\sigma)(t) := \gamma(t)\sigma(t).$$

Show that (for $t \in (a, b)$)

$$(\gamma \sigma)^{\cdot}(t) = \gamma(t)\dot{\sigma}(t) + \dot{\gamma}(t)\sigma(t).$$

♦ Exercise 224

(a) Let $\gamma: (-1,1) \to \mathbb{R}^{3 \times 3}$ be given by

$$\gamma(t) := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos t & \sin t \\ 0 & -\sin t & \cos t \end{bmatrix}.$$

Show that γ is a curve in SO(3) and find $\dot{\gamma}(0)$. Show that

$$(\gamma^2)^{\cdot}(0) = 2\dot{\gamma}(0).$$

(b) Let $\sigma: (-1,1) \to \mathbb{R}^{3 \times 3}$ be given by

$$\sigma(t) := \begin{bmatrix} 0 & 0 & 0 \\ 0 & \cos t & \sin t \\ 0 & -\sin t & \cos t \end{bmatrix}.$$

Calculate $\dot{\sigma}(0)$. Write the matrix $\gamma(t)\sigma(t)$ and verify that

$$(\gamma\sigma)^{\cdot}(0) = \dot{\gamma}(0) + \dot{\sigma}(0).$$

 \diamond **Exercise 225** Let $\alpha: (-1,1) \to \mathbb{C}^{n \times n}$ be given by

$$\alpha(t) := \begin{bmatrix} e^{i\pi t} & 0 \\ 0 & e^{i\frac{\pi t}{2}} & 0 \\ 0 & 0 & e^{i\frac{\pi t}{2}} \end{bmatrix}.$$

Show that α is a curve in U(3). Calculate $\dot{\alpha}(0)$.

4.4.5 DEFINITION. The **tangent space** to (the matrix group) G at $A \in G$ is the set

$$T_A G := \{ \dot{\gamma}(0) \in \mathbb{k}^{n \times n} \, | \, \gamma \text{ is a curve in } G \text{ with } \gamma(0) = A \}.$$

4.4.6 PROPOSITION. The set $T_A G$ is a real vector subspace of $\mathbb{k}^{n \times n}$. PROOF : Let $\alpha, \beta : (a, b) \to \mathbb{k}^{n \times n}$ be two curves in G through A (i.e., $\alpha(0) = \beta(0) = A$). Then

$$\gamma: (a,b) \to \mathbb{k}^{n \times n}, \quad t \mapsto \alpha(t) A^{-1} \beta(t)$$

is also a curve in G with $\gamma(0) = A$. We have

$$\dot{\gamma}(t) = \dot{\alpha}(t)A^{-1}\beta(t) + \alpha(t)A^{-1}\dot{\beta}(t)$$

and hence

$$\dot{\gamma}(0) = \dot{\alpha}(0)A^{-1}\beta(0) + \alpha(0)A^{-1}\dot{\beta}(0) = \dot{\alpha}(0) + \dot{\beta}(0)$$

which shows that $T_A G$ is closed under (vector) addition.

Similarly, if $\lambda \in \mathbb{R}$ and $\alpha : (a, b) \to \mathbb{k}^{n \times n}$ is a curve in G with $\alpha(0) = A$, then

$$\eta: (a,b) \to \mathbb{k}^{n \times n}, \quad t \mapsto \alpha(\lambda t)$$

is another such curve. Since

$$\dot{\eta}(0) = \lambda \dot{\alpha}(0)$$

we see that $T_A G$ is closed under (real) scalar multiplication. So $T_A G$ is a (real) vector subspace of $\mathbb{k}^{n \times n}$.

NOTE : Since the vector space $\mathbb{k}^{n \times n}$ is *finite dimensional*, so is (the tangent space) $T_A G$.

4.4.7 DEFINITION. If $G \leq GL(n, \mathbb{k})$ is a matrix group, its **dimension** is the dimension of the (real) vector space $T_I G$ (I is the identity matrix). So

$$\dim G := \dim_{\mathbb{R}} T_I G.$$

NOTE : If the matrix group G is complex, then its *complex dimension* is

$$\dim_{\mathbb{C}} G := \dim_{\mathbb{C}} T_I G.$$

 \diamond Exercise 226 Show that the matrix group U(1) has dimension 1.

NOTE : The *only* connected matrix groups (up to isomorphism) of dimension 1 are $\mathbb{T}^1 = \mathsf{U}(1)$ and \mathbb{R} , and of dimension 2 are $\mathbb{R}^2, \mathbb{T}^1 \times \mathbb{R}, \mathbb{T}^2$, and $\mathsf{GA}^+(1, \mathbb{R})$.

4.4.8 EXAMPLE. The real general linear group $\mathsf{GL}(n,\mathbb{R})$ has dimension n^2 .

The determinant function det : $\mathbb{R}^{n \times n} \to \mathbb{R}$ is *continuous* and det (I) = 1. So there is some ϵ -ball about I in $\mathbb{R}^{n \times n}$ such that for each A in this ball det $(A) \neq 0$ (i.e., $A \in \mathsf{GL}(n,\mathbb{R})$). If $B \in \mathbb{R}^{n \times n}$, then define a curve σ in $\mathbb{R}^{n \times n}$ by

$$\sigma(t) := tB + I.$$

Then $\sigma(0) = I$ and $\dot{\sigma}(0) = B$, and (for small t) $\sigma(t) \in \mathsf{GL}(n, \mathbb{R})$. Hence the tangent space $T_I \mathsf{GL}(n, \mathbb{R})$ is all of $\mathbb{R}^{n \times n}$ which has dimension n^2 . So

$$\dim \mathsf{GL}\left(n,\mathbb{R}\right) = n^2.$$

♦ **Exercise 227** Show that the dimension of the *complex* general linear group $\mathsf{GL}(n, \mathbb{C})$ is $2n^2$.

4.4.9 PROPOSITION. Let $\mathsf{Sk-sym}(n)$ denote the set of all skew-symmetric matrices in $\mathbb{R}^{n \times n}$. Then $\mathsf{Sk-sym}(n)$ is a linear subspace of $\mathbb{R}^{n \times n}$ and its dimension is $\frac{n(n-1)}{2}$.

PROOF : If $A, B \in \mathsf{Sk-sym}(n)$, then

$$(A+B)^{\top} + (A+B) = A^{\top} + A + B^{\top} + B = 0$$

so that $\mathsf{Sk-sym}(n)$ is closed under (vector) addition.

It is also closed under scalar multiplication, for if $A \in \mathsf{Sk-sym}(n)$ and $\lambda \in \mathbb{R}$, then $(\lambda A)^{\top} = \lambda A^{\top}$ so that

$$(\lambda A)^{\top} + \lambda A = \lambda (A^{\top} + A) = 0.$$

To check the dimension of $\mathsf{Sk-sym}(n)$ we construct a basis. Let E_{ij} denote the matrix whose entries are all zero except the *ij*-entry, which is 1, and the *ji*-entry, which is -1. If we define these E_{ij} only for i < j, we can see that they form a *basis* for $\mathsf{Sk-sym}(n)$.

It is easy to compute that there are

$$(n-1) + (n-2) + \dots + 2 + 1 = \frac{n(n-1)}{2}$$

of them.

♦ **Exercise 228** Show that if σ is a curve through the identity (i.e., $\sigma(0) = I$) in the orthogonal group O(n), then $\dot{\sigma}(0)$ is skew-symmetric.

NOTE : It follows that dim $O(n) \le \frac{n(n-1)}{2}$. Later we will show that this evaluation is an equality.

♦ **Exercise 229** A matrix $A \in \mathbb{C}^{n \times n}$ is called *skew-Hermitian* if $A^* + A = 0$.

- (a) Show that the diagonal terms of a skew-Hermitian matrix are purely imaginary and hence deduce that the set Sk-Herm (n) of all skew-Hermitian matrices in $\mathbb{C}^{n \times n}$ is *not* a vector space over \mathbb{C} .
- (b) Prove that Sk-Herm(n) is a *real* vector space of dimension

$$n+2\,\frac{n(n-1)}{2} = n^2.$$

(c) If σ is a curve through the identity in U(n), show that $\dot{\sigma}(0)$ is skew-Hermitian an hence

dim $U(n) \le n^2$.

We will adopt the notation $\mathfrak{g} := T_I G$ for this real vector subspace of $\mathbb{k}^{n \times n}$. In fact, \mathfrak{g} has a more interesting algebraic structure, namely that of a *Lie algebra*.

NOTE : It is customary to use *lower case Gothic* (Fraktur) characters (such as $\mathfrak{a}, \mathfrak{g}$ and \mathfrak{h}) to refer to Lie algebras.

4.4.10 DEFINITION. A (real) Lie algebra \mathfrak{a} is a real vector space equipped with a product

$$[\cdot, \cdot] : \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a}, \quad (x, y) \mapsto [x, y]$$

such that (for $\lambda, \mu \in \mathbb{R}$ and $x, y, z \in \mathfrak{a}$)

- (LA1) [x, y] = -[y, x].
- (LA2) $[\lambda x + \mu y, z] = \lambda[x, z] + \mu[y, z].$
- (LA3) [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.

The product $[\cdot, \cdot]$ is called the *Lie bracket* of the Lie algebra \mathfrak{a} .

NOTE: (1) Condition (LA3) is called the *Jacobi identity*. So the Lie bracket $[\cdot, \cdot]$ of (the Lie algebra) \mathfrak{a} is a *skew-symmetric bilinear* mapping (on \mathfrak{a}) which satisfies the Jacobi identity. Hence Lie algebras are *nonassociative* algebras. The Lie bracket plays for Lie algebras the same role that the associative law plays for associative algebras.

(2) While we can define *complex* Lie algebras (or, more generally, Lie algebras over any field), we shall only consider Lie algebras over the real field \mathbb{R} .

4.4.11 EXAMPLE. Let $\mathfrak{a} = \mathbb{R}^n$ and set (for all $x, y \in \mathbb{R}^n$)

$$[x,y] := 0.$$

The trivial product is a skew-symmetric bilinear multiplication (on \mathbb{R}^n) which satisfies the Jacobi identity and hence is a Lie bracket. \mathbb{R}^n equipped with this product (Lie bracket) is a Lie algebra. Such a Lie algebra is called an *Abelian Lie algebra*. \diamond **Exercise 230** Show that the *only* Lie algebra structure on (the vector space) \mathbb{R} is the trivial one.

4.4.12 EXAMPLE. Let $\mathfrak{a} = \mathbb{R}^3$ and set (for $x, y \in \mathbb{R}^3$)

 $[x, y] := x \times y$ (the cross product).

For the standard unit vectors e_1, e_2, e_3 we have

$$[e_1, e_2] = -[e_2, e_1] = e_3, \quad [e_2, e_3] = -[e_3, e_2] = e_1, \quad [e_3, e_1] = -[e_1, e_3] = e_2.$$

Then \mathbb{R}^3 equipped with this bracket operation is a Lie algebra. In fact, as we will see later, this is the Lie algebra of (the matrix group) SO(3) and also of SU(2) in disguise.

Given two matrices $A, B \in \mathbb{k}^{n \times n}$, their **commutator** is

$$[A, B] := AB - BA.$$

A and B commute (i.e., AB = BA) if and only if [A, B] = 0. The commutator $[\cdot, \cdot]$ is a product on $\mathbb{k}^{n \times n}$ satisfying conditions (LA1)-(LA3).

 \diamond Exercise 231 Verify the *Jacobi identity* for the commutator $[\cdot, \cdot]$.

The *real* vector space $\mathbb{k}^{n \times n}$ equipped with the commutator $[\cdot, \cdot]$ is a Lie algebra.

NOTE: The procedure to give $\Bbbk^{n \times n}$ a Lie algebra structure can be extended to any *associative* algebra. A Lie product (bracket) can be defined in any associative algebra by the comutator [x, y] = xy - yx, making it a Lie algebra. Here the skew-symmetry condition (axiom) is clearly satisfied, and one can check easily that in this case the Jacobi identity for the commutator follows from the associativity law for the ordinary product.

There is another way in which Lie algebras arise in the study of algebras. A *derivation* d of a *nonassociative* algebra \mathcal{A} (i.e., a vector space endowed with a bilinear mapping $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$) is a linear mapping $\mathcal{A} \to \mathcal{A}$ satisfying the formal analogue of the Leibniz rule for differentiating a product (for all $x, y \in \mathcal{A}$)

$$d(xy) = (dx)y + x(dy).$$

(The concept of a derivation is an abstraction of the idea of a first order differential operator.) The set of all derivations on \mathcal{A} is clearly a vector subspace of the algebra End (\mathcal{A}) of all linear mappings $\mathcal{A} \to \mathcal{A}$. Although the product of derivations is in general not a derivation, the commutator $d_1d_2 - d_2d_1$ of two derivations is again a derivation. Thus the set of all derivations of a nonassociative algebra is a Lie algebra, called the *derivation algebra* of the given nonassociative algebra.

Suppose that \mathfrak{a} is a vector subspace of the Lie algebra $\mathbb{k}^{n \times n}$. Then \mathfrak{a} is a *Lie subalgebra* of $\mathbb{k}^{n \times n}$ if it is *closed* under taking commutators of pairs of alements in \mathfrak{a} ; that is,

$$A, B \in \mathfrak{a} \Rightarrow [A, B] \in \mathfrak{a}$$

Of course, $\mathbb{k}^{n \times n}$ is a Lie subalgebra of itself.

4.4.13 THEOREM. If $G \leq \mathsf{GL}(n, \Bbbk)$ is a matrix group, then the tangent space $\mathfrak{g} = T_I G$ (at the identity) is a Lie subalgebra of $\Bbbk^{n \times n}$.

PROOF : We will show that two curves α, β in G with $\alpha(0) = \beta(0) = I$, there is such a curve γ with $\dot{\gamma}(0) = [\dot{\alpha}(0), \dot{\beta}(0)]$.

Consider the mapping

$$F: (s,t) \mapsto F(s,t) := \alpha(s)\beta(t)\alpha(s)^{-1}.$$

This is clearly (continuous and) differentiable with respect to each of the variables s, t. For each s (in the domain of α), $F(s, \cdot)$ is a curve in G with F(s, 0) = I. Differentiating gives

$$\left. \frac{d}{dt} F(s,t) \right|_{t=0} = \alpha(s)\dot{\beta}(0)\alpha(s)^{-1}$$

and so

$$\alpha(s)\dot{\beta}(0)\alpha(s)^{-1} \in \mathfrak{g}.$$

Since \mathfrak{g} is a *closed subspace* of $\mathbb{k}^{n \times n}$ (Any vector subspace is an intersection of hyperplanes), whenever this limit exists we also have

$$\lim_{s \to 0} \frac{1}{s} \left(\alpha(s) \dot{\beta}(0) \alpha(s)^{-1} - \dot{\beta}(0) \right) \in \mathfrak{g}.$$

 \diamond **Exercise 232** Verify the following (matrix version of the) usual rule for differentiating an inverse :

$$\frac{d}{dt}\left(\alpha(t)^{-1}\right) = -\alpha(t)^{-1}\dot{\alpha}(t)\alpha(t)^{-1}.$$

We have

$$\begin{split} \lim_{s \to 0} \frac{1}{s} \left(\alpha(s) \dot{\beta}(0) \alpha(s)^{-1} - \dot{\beta}(0) \right) &= \left. \frac{d}{ds} \alpha(s) \dot{\beta}(0) \alpha(s)^{-1} \right|_{s=0} \\ &= \left. \dot{\alpha}(0) \dot{\beta}(0) \alpha(0) - \alpha(0) \dot{\beta}(0) \alpha(0)^{-1} \dot{\alpha}(0) \alpha(0)^{-1} \\ &= \left. \dot{\alpha}(0) \dot{\beta}(0) \alpha(0) - \alpha(0) \dot{\beta}(0) \dot{\alpha}(0) \right. \\ &= \left. \dot{\alpha}(0) \dot{\beta}(0) - \dot{\beta}(0) \dot{\alpha}(0) \right. \\ &= \left. \left. \left. \dot{\alpha}(0) \dot{\beta}(0) - \dot{\beta}(0) \dot{\alpha}(0) \right. \right] \end{split}$$

This shows that $[\dot{\alpha}(0), \dot{\beta}(0)] \in \mathfrak{g}$, hence it must be of the form $\dot{\gamma}(0)$ for some curve.

So for each matrix group G there is a Lie algebra $\mathfrak{g} = T_I G$. We call \mathfrak{g} the **Lie algebra** of G.

NOTE : The essential phenomenon behind Lie theory is that one may associate in a natural way to a matrix group G its Lie algebra \mathfrak{g} . The Lie algebra is first of all a (real) vector space and secondly is endowed with a skew-symmetric bilinear product (called the Lie bracket or commutator). Amazingly, the group G is almost completely determined by \mathfrak{g} and its Lie bracket. Thus for many purposes one can replace G with \mathfrak{g} . Since G is a complicated nonlinear object and \mathfrak{g} is just a vector space, it is usually vastly simpler to work with \mathfrak{g} . Otherwise intractable computations may become straightforward linear algebra. This is one source of the power of Lie theory.

Homomorphisms of Lie algebras

A suitable type of homomorphism $G \to H$ between matrix groups gives rise to a linear mapping $\mathfrak{g} \to \mathfrak{h}$ respecting the Lie algebra structures. **4.4.14** DEFINITION. Let $G \leq \mathsf{GL}(n, \Bbbk), H \leq \mathsf{GL}(m, \Bbbk)$ be matrix groups and let $\varphi : G \to H$ be a continuous mapping. Then φ is said to be **differentiable** if for every (differentiable) curve $\gamma : (a, b) \to G$, the composite mapping $\varphi \circ \gamma : (a, b) \to H$ is a (differentiable) curve with derivative

$$(\varphi \circ \gamma)^{\cdot}(t) = \frac{d}{dt}\varphi(\gamma(t))$$

and if whenever two (differentiable) curves $\alpha, \beta : (a, b) \to G$ both satisfy the conditions

$$\alpha(0) = \beta(0)$$
 and $\dot{\alpha}(0) = \dot{\beta}(0)$

then

$$(\varphi \circ \alpha)^{\cdot}(0) = (\varphi \circ \beta)^{\cdot}(0).$$

Such a mapping φ is a *differentiable homomorphism* if it is also a group homomorphism. A continuous homomorphism of matrix groups that is also *differentiable* is called a **Lie homomorphism**.

NOTE : The "technical restriction" in the definition of a Lie homomorphism is in fact *unnecessary*.

If $\varphi : G \to H$ is the restriction of a differentiable mapping $\Phi : \mathsf{GL}(n, \Bbbk) \to \mathsf{GL}(m, \Bbbk)$, then φ is also a differentiable mapping.

4.4.15 PROPOSITION. Let G, H, K be matrix groups and $\varphi : G \to H, \psi : H \to K$ be differentiable homomorphisms.

(a) For each $A \in G$ there is a linear mapping $d\varphi_A : T_A G \to T_{\varphi(A)} H$ given by

$$d\varphi_A(\dot{\gamma}(0)) = (\varphi \circ \gamma)^{\cdot}(0).$$

(b) We have

$$d\psi_{\varphi(A)} \circ d\varphi_A = d(\psi \circ \varphi)_A.$$

(c) For the identity mapping $id_G: G \to G$ and $A \in G$,

$$d \, id_G = id_{T_AG}.$$

207

PROOF: (a) The definition of $d\varphi_A$ makes sense since (by the definition of differentiability), given $X \in T_A G$, for any curve γ with

$$\gamma(0) = A$$
 and $\dot{\gamma}(0) = X$

 $(\varphi \circ \gamma)^{\cdot}(0)$ depends only on X and not on γ .

 \diamond Exercise 233 Verify that the maping $d\varphi_A : T_A G \to T_{\varphi(A)} H$ is linear.

The identities (b) and (c) are straightforward to verify.

If $\varphi : G \to H$ is a differentiable homomorphism, then (since $\varphi(I) = I$) $d\varphi_I : T_I G \to T_I H$ is a linear mapping, called the **derivative** of φ and usually denoted by

$$d\varphi:\mathfrak{g}\to\mathfrak{h}.$$

4.4.16 DEFINITION. Let $\mathfrak{g}, \mathfrak{h}$ be Lie algebras. A linear mapping $\Phi : \mathfrak{g} \to \mathfrak{h}$ is a **homomorphism of Lie algebras** if (for $x, y \in \mathfrak{g}$)

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

4.4.17 THEOREM. Let G, H be matrix groups and $\varphi : G \to H$ be a Lie homomorphism. Then the derivative $d\varphi : \mathfrak{g} \to \mathfrak{h}$ is a homomorphism of Lie algebras.

PROOF: Following ideas and notation in the proof of THEOREM 4.4.13, for curves α, β in G with $\alpha(0) = \beta(0) = I$, we can use the composite mapping

$$\varphi \circ F : (s,t) \mapsto \varphi(F(s,t)) = \varphi(\alpha(s))\varphi(\beta(t))\varphi(\alpha(s))^{-1}$$

to deduce

$$d\varphi([\dot{\alpha}(0), \dot{\beta}(0)]) = [d\varphi(\dot{\alpha}(0)), d\varphi(\dot{\beta}(0))].$$

4.4.18 COROLLARY. Let G, H be matrix groups and $\varphi : G \to H$ be an isomorphism of matrix groups. Then the derivative $d\varphi : \mathfrak{g} \to \mathfrak{h}$ is an isomorphism of Lie algebras.

PROOF : $\varphi^{-1} \circ \varphi$ is the identity, so

$$d\varphi^{-1} \circ d\varphi : T_I G \to T_I G$$

is the identity. Thus $d\varphi^{-1}$ is surjective and $d\varphi$ is injective.

Likewise, $\varphi \circ \varphi^{-1}$ is the identity, so $d\varphi \circ d\varphi^{-1}$ is the identity. Thus $d\varphi^{-1}$ is injective, and $d\varphi$ is surjective. The result now follows.

NOTE : Isomorphic matrix groups have isomorphic Lie algebras. The converse (i.e., matrix groups with isomorphic Lie algebras are isomorphic) is *false*. For example, the rotation group SO(2) and the diagonal group

$$D_{1} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & e^{a} \end{bmatrix} \mid a \in \mathbb{R} \right\} \leq \mathsf{GA}^{+}(1, \mathbb{R})$$

have both Lie algebras isomorphic to \mathbb{R} (the only Lie algebra structure on \mathbb{R}), but SO(2) is homeomorphic to a circle, while D_1 is homeomorphic to \mathbb{R} , so they are certainly *not* isomorphic.

However, the converse is - in a sense - almost true, so that the bracket operation on \mathfrak{g} almost determine G as a group. After the existence of the Lie algebra, this fact is the most remarkable in Lie theory. Its precise formulation is known as *Lie's Third Theorem*.

4.5 More Properties of the Exponential Mapping

The following formula can be considered as another definition of the matrix exponential.

4.5.1 PROPOSITION. Let $A \in \mathbb{k}^{n \times n}$. Then

$$\exp(A) = \lim_{r \to \infty} \left(I + \frac{1}{r}A\right)^r.$$

PROOF : Consider the difference

$$\exp\left(A\right) - \left(I + \frac{1}{r}A\right)^r = \sum_{k=0}^{\infty} \left(\frac{1}{k!} - \frac{1}{r^k} \binom{r}{k}\right) A^k.$$

This matrix series converges since the series for the matrix exponential $\exp(A)$ converges and $\left(I + \frac{1}{r}A\right)^r$ is a polynomial. The coefficients in the rhs are nonnegative since

$$\frac{1}{k!} \ge \frac{r(r-1)\cdots(r-k+1)}{r\cdot r\cdots r} \frac{1}{k!}.$$

Therefore, setting ||A|| = a, we get

$$\left\|\exp\left(A\right) - \left(I + \frac{1}{r}A^r\right)^r\right\| \le \sum_{k=0}^{\infty} \left(\frac{1}{k!} - \frac{1}{r^k}\binom{r}{k}\right)a^k = e^a - \left(1 + \frac{a}{r}\right)^r$$

where the expression on the right approaches zero (as $r \to \infty$). The result now follows.

4.5.2 Proposition. Let $A \in \mathbb{k}^{n \times n}$ and $\epsilon \in \mathbb{R}$. Then

$$\det (I + \epsilon A) = 1 + \epsilon \operatorname{tr} A + O(\epsilon^2) \quad (as \ \epsilon \to 0).$$

PROOF: The determinant of $I + \epsilon A$ equals the product of the eigenvalues of the matrix. But the eigenvalues of $I + \epsilon A$ (with due regard for multiplicity) equal $1 + \epsilon \lambda_i$, where the λ_i are the eigenvalues of A. It follows that

$$\det (I + \epsilon A) = (1 + \epsilon \lambda_1)(1 + \epsilon \lambda_2) \cdots (1 + \epsilon \lambda_n)$$

= $1 + \epsilon (\lambda_1 + \lambda_2 + \cdots + \lambda_n) + O(\epsilon^2)$
= $1 + \epsilon \operatorname{tr} A + O(\epsilon^2).$

NOTE : Whenever we have a mapping Z from some (open) interval (a, b), a < 0 < b into a finite-dimensional normed vector space (e.g. $\mathbb{k}^{n \times n}$), then Z will often be denoted by $O(t^k)$ if $t \mapsto \frac{1}{t^k}Z(t)$ is bounded in an (open) neighborhood of the origin 0 (i.e. there are constants C_1 and C_2 such that

$$||Z(t)|| \le C_1 |t^k|$$
 for $|t| < C_2$.)

Thus $O(t^k)$ may denote different mappings at different times. The big-O notation was first introduced in 1892 by PAUL G.H. BACHMANN (1837-1920) in a book on number theory, and is currently used in several areas of mathematics and computer science (including mathematical analysis and the theory of algorithms).

The following result is useful.

4.5.3 LEMMA. Let $\alpha : (a, b) \to \mathbb{k}^{n \times n}$ be a curve. Then

$$\left. \frac{d}{dt} \det \alpha(t) \right|_{t=0} = \operatorname{tr} \dot{\alpha}(0).$$

PROOF : The operation $\partial := \frac{d}{dt}\Big|_{t=0}$ has the *derivation property*

$$\partial(\gamma_1\gamma_2) = (\partial\gamma_1)\gamma_2(0) + \gamma_1(0)\partial\gamma_2.$$

Put $\alpha(t) = \begin{bmatrix} a_{ij} \end{bmatrix}$ and notice that (when t = 0) $a_{ij} = \delta_{ij}$. Write C_{ij} for the *cofactor matrix* obtained from $\alpha(t)$ by deleting the *i*th row and the *j*th column. By expanding along the *n*th row we get

det
$$\alpha(t) = \sum_{j=1}^{n} (-1)^{n+j} a_{nj} \det C_{nj}.$$

For t = 0 (since $\alpha(0) = I$) we have

det
$$C_{nj} = \delta_{nj}$$

Then

$$\partial \det \alpha(t) = \sum_{j=1}^{n} (-1)^{n+j} ((\partial a_{nj}) \det C_{nj} + a_{nj} (\partial \det C_{nj}))$$
$$= \sum_{j=1}^{n} (-1)^{n+j} ((\partial a_{nj}) \det C_{nj}) + (\partial \det C_{nn})$$
$$= \partial a_{nn} + \partial \det C_{nn}.$$

We can repeat this calculation with the $(n-1) \times (n-1)$ matrix C_{nn} and so on. This gives

$$\partial \det \alpha(t) = \partial a_{nn} + \partial a_{n-1,n-1} + \partial \det C_{n-1,n-1}$$

$$\vdots$$

$$= \partial a_{nn} + \partial a_{n-1,n-1} + \dots + \partial a_{11}$$

$$= \operatorname{tr} \dot{\alpha}(0).$$

We can now prove a remarkable (and very useful) result, known as *Liou*ville's Formula. Three different proofs will be given.

4.5.4 THEOREM. (LIOUVILLE'S FORMULA) For $A \in \mathbb{k}^{n \times n}$ we have

$$\det \exp\left(A\right) = e^{\operatorname{tr} A}.$$

FIRST SOLUTION (using the second definition of the exponential) : We have

det
$$\exp(A) = \det \lim_{r \to \infty} \left(I + \frac{1}{r}A\right)^r = \lim_{r \to \infty} \det \left(I + \frac{1}{r}A\right)^r$$

since the determinant function det : $\mathbb{k}^{n \times n} \to \mathbb{k}$ is *continuous*. Moreover, by PROPOSITION 4.5.2,

$$\det\left(I + \frac{1}{r}A\right)^r = \left[\det\left(I + \frac{1}{r}A\right)\right]^r = \left[1 + \frac{1}{r}\operatorname{tr} A + O\left(\frac{1}{r^2}\right)\right]^r \text{ (as } r \to \infty\text{)}.$$

It only remains to note that (for any $a \in \mathbb{k}$)

$$\lim_{r \to \infty} \left[1 + \frac{a}{r} + O\left(\frac{1}{r^2}\right) \right]^r = e^a$$

In particular, for $a = \operatorname{tr} A$, we get the desired result.

SECOND SOLUTION (using differential equations) : Consider the curve

$$\gamma: \mathbb{R} \to \mathsf{GL}\left(1, \Bbbk\right) = \Bbbk^{\times}, \quad t \mapsto \det \, \exp \, (tA).$$

Then (by LEMMA 4.5.3 applied to the curve γ)

$$\begin{split} \dot{\gamma}(t) &= \lim_{h \to 0} \frac{1}{h} \left[\det \exp\left((t+h)A\right) - \det \exp\left(tA\right) \right] \\ &= \det \exp\left(tA\right) \lim_{h \to 0} \frac{1}{h} \left[\det \exp\left(hA\right) - 1 \right] \\ &= \det \exp\left(tA\right) \operatorname{tr} A \\ &= \gamma(t) \operatorname{tr} A. \end{split}$$

So γ satisfies the same differential equation and initial condition as the curve $t \mapsto e^{t \operatorname{tr} A}$. By the uniqueness of the solution (see **Exercise 219**), it follows that

$$\gamma(t) = \det \exp\left(tA\right) = e^{t \operatorname{tr} A}.$$

In particular, for t = 1, we get the desired result.

THIRD SOLUTION (using Jordan canonical form) : If $B \in GL(n, \Bbbk)$, then (see **Exercise 221**)

$$\det \exp (BAB^{-1}) = \det (B \exp (A)B^{-1})$$
$$= \det B \cdot \det \exp(A) \cdot \det B^{-1}$$
$$= \det \exp (A)$$

and

$$e^{\operatorname{tr}(BAB^{-1})} = e^{\operatorname{tr}A}.$$

So it suffices to prove the identity for BAB^{-1} for a suitably chosen invertible matrix B. Using for example the theory of Jordan canonical forms, there is a suitable choice of such a B for which

$$BAB^{-1} = D + N$$

with D diagonal and N strictly upper triangular (i.e., $N_{ij} = 0$ for $i \ge j$). Then N is nilpotent (i.e., $N^k = O$ for some $k \ge 1$). We have

$$\exp(BAB^{-1}) = \sum_{k=0}^{\infty} \frac{1}{k!} (D+N)^k$$

= $\sum_{k=0}^{\infty} \frac{1}{k!} D^k + \sum_{k=0}^{\infty} \frac{1}{(k+1)!} \left((D+N)^{k+1} - D^{k+1} \right)$
= $\exp(D) + \sum_{k=0}^{\infty} \frac{1}{(k+1)!} N(D^k + D^{k-1}N + \dots + N^k).$

The matrix

$$N(D^k + D^{k-1}N + \dots + N^k)$$

is strictly upper triangular, and so

$$\exp\left(BAB^{-1}\right) = \exp\left(D\right) + N'$$

where N' is strictly upper triangular. Now, if $D = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$, we

have

$$det \exp (A) = det \exp (BAB^{-1})$$

$$= det \exp (D)$$

$$= det diag (e^{\lambda_1}, e^{\lambda_2}, \dots, e^{\lambda_n})$$

$$= e^{\lambda_1} e^{\lambda_2} \cdots e^{\lambda_n}$$

$$= e^{\lambda_1 + \lambda_2 + \dots + \lambda_n}$$

$$= e^{\operatorname{tr} D}$$

$$= e^{\operatorname{tr} (BAB^{-1})}$$

$$= e^{\operatorname{tr} A}.$$

The exponential mapping

$$\exp: \mathbb{k}^{n \times n} \to \mathsf{GL}\left(n, \mathbb{k}\right)$$

is a basic link between the linear structure on $\mathbb{k}^{n \times n}$ and the multiplicative structure on $\mathsf{GL}(n,\mathbb{k})$. Let G be a matrix subgroup of $\mathsf{GL}(n,\mathbb{k})$. Applying PROPOSITION 4.3.3, we may choose $\rho \in \mathbb{R}$ so that $0 < \rho \leq \frac{1}{2}$ and if $A, B \in \mathcal{B}_{\mathbb{k}^{n \times n}}(O,\rho)$, then $\exp(A)\exp(B) \in \exp\left(\mathcal{B}_{\mathbb{k}^{n \times n}}(O,\frac{1}{2})\right)$. Since exp is one-toone on $\mathcal{B}_{\mathbb{k}^{n \times n}}(O,\rho)$, there is a unique matrix $C \in \mathbb{k}^{n \times n}$ for which

$$\exp\left(A\right)\exp\left(B\right) = \exp\left(C\right).$$

NOTE: There is a beautiful formula, the *Baker-Campbell-Hausdorff formula* which expresses C as a universal power series in A and B. To develop this completely would take too long. Specifically, (one form of) the B-C-H formula says that *if* X and Y are sufficiently small, then

$$\exp(X)\exp(Y) = \exp(Z)$$
 with
 $Z = X + Y + \frac{1}{2}[X, Y] + \frac{1}{12}[X, [X, Y]] - \frac{1}{12}[Y, [X, Y]] + \cdots$

It is not supposed to be evident at the moment what "..." refers to. The only important point is that all the terms (in the expansion of Z) are given in terms of X

and Y, Lie brackets of X and Y, Lie brackets of Lie brackets involving X and Y, etc. Then it follows that the mapping $\phi: G \to \mathsf{GL}(n, \mathbb{R})$ "defined" by the relation

$$\phi\left(\exp(X)\right) = \exp\left(\phi(X)\right)$$

is such that on elements of the form $\exp(X)$, with X sufficiently small, is a group homomorphism. Hence the B-C-H formula shows that all the information about the group product, a least near the identity, is "encoded" in the Lie algebra.

An interesting special case is the following : If $X, Y \in \mathbb{C}^{n \times n}$ and X, Y commute with their commutator (i.e., [X, [X, Y]] = [Y, [X, Y]), then

$$\exp(X)\exp(Y) = \exp\left(X + Y + \frac{1}{2}[X,Y]\right).$$

 \diamond Exercise 234 Show by direct computation that for

$$X, Y \in \mathfrak{heis} = \left\{ egin{bmatrix} 0 & a & b \ 0 & 0 & c \ 0 & 0 & 0 \end{bmatrix} \mid a, b, c \in \mathbb{R}
ight\}$$

(the Lie algebra of the Heisenberg group Heis)

$$\exp(X)\exp(Y) = \exp\left(X + Y + \frac{1}{2}[X,Y]\right).$$

We set

$$R = C - A - B \in \mathbb{k}^{n \times n}.$$

For $X \in \mathbb{k}^{n \times n}$, we have

$$\exp\left(X\right) = I + X + R_1(X),$$

where the remainder term $R_1(X)$ is given by

$$R_1(X) = \sum_{k=2}^{\infty} \frac{1}{k!} X^k.$$

Hence

$$||R_1(X)|| \le ||X||^2 \sum_{k=2}^{\infty} \frac{1}{k!} ||X||^{k-2}$$

and therefore if ||X|| < 1, then

$$||R_1(X)|| \le ||X||^2 \sum_{k=2}^{\infty} \frac{1}{k!} = ||X||^2 (e-2) < ||X||^2.$$

Now for $X = C \in \mathcal{B}_{\mathbb{k}^{n \times n}}(O, \frac{1}{2})$, we have

$$\exp\left(C\right) = I + C + R_1(C)$$

with

$$||R_1(C)|| < ||C||^2.$$

Similar considerations lead to

$$\exp(C) = \exp(A)\exp(B) = I + A + B + R_1(A, B),$$

where

$$R_1(A,B) = \sum_{k=2}^{\infty} \frac{1}{k!} \left(\sum_{r=0}^k \binom{k}{r} A^r B^{k-r} \right).$$

This gives

$$\begin{aligned} \|R_1(A,B)\| &\leq \sum_{k=2}^{\infty} \frac{1}{k!} \left(\sum_{r=0}^k \binom{k}{r} \|A\|^r \|B\|^{k-r} \right) \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \left(\|A\| + \|B\| \right)^k \\ &= \left(\|A\| + \|B\| \right)^2 \sum_{k=2}^{\infty} \frac{1}{k!} \left(\|A\| + \|B\| \right)^{k-2} \\ &\leq \left(\|A\| + \|B\| \right)^2 \end{aligned}$$

since ||A|| + ||B|| < 1.

Combining the two ways of writing $\exp(C)$ from above, we have

$$C = A + B + R_1(C) - R_1(A, B)$$

and so

$$\begin{aligned} \|C\| &\leq \|A\| + \|B\| + \|R_1(A, B)\| + \|R_1(C)\| \\ &< \|A\| + \|B\| + (\|A\| + \|B\|)^2 + \|C\|^2 \\ &\leq 2(\|A\| + \|B\|) + \frac{1}{2}\|C\| \end{aligned}$$

since $||A||, ||B||, ||C|| \leq \frac{1}{2}$. Finally this gives

$$||C|| \le 4 \left(||A|| + ||B|| \right).$$

We also have

$$||R|| = ||C - A - B|| \leq ||R_1(A, B)|| + ||R_1(C)||$$

$$\leq (||A|| + ||B||)^2 + (4(||A|| + ||B||))^2$$

$$= 17 (||A|| + ||B||)^2.$$

We have proved the following result.

4.5.5 PROPOSITION. Let $A, B, C \in \mathcal{B}_{\mathbb{k}^{n \times n}}(O, \frac{1}{2})$ such that $\exp(A) \exp(B) = \exp(C)$. Then C = A + B + R, where the remainder term R satisfies

$$||R|| \le 17 (||A|| + ||B||)^2$$

We can refine this estimate (to second order). We only point out the essential steps (details will be omitted). Set

$$S=C-A-B-\frac{1}{2}[A,B]\in \Bbbk^{n\times n}$$

and write

$$\exp(C) = I + C + \frac{1}{2}C^2 + R_2(C)$$

with

$$||R_2(C)|| \le \frac{1}{3} ||C||^3.$$

Then

$$\exp(C) = I + A + B + \frac{1}{2}[A, B] + S + \frac{1}{2}C^2 + R_2(C)$$
$$= I + A + B + \frac{1}{2}(A^2 + 2AB + B^2) + T,$$

where

$$T = S + \frac{1}{2}(C^2 - (A+B)^2) + R_2(C).$$

Also

$$\exp(A)\exp(B) = I + A + B + \frac{1}{2}(A^2 + 2AB + B^2) + R_2(A, B)$$

with

$$||R_2(A,B)|| \le \frac{1}{3} (||A|| + ||B||)^3.$$

We see that

$$S = R_2(A, B) + \frac{1}{2}((A + B)^2 - C^2) - R_2(C)$$

and by taking norms we get

$$||S|| \leq ||R_2(A,B)|| + \frac{1}{2}||(A+B)(A+B-C) + (A+B-C)C|| + ||R_2(C)||$$

$$\leq \frac{1}{3}(||A|| + ||B||)^3 + \frac{1}{2}(||A|| + ||B|| + ||C||)||A+B-C|| + \frac{1}{3}||C||^3$$

$$\leq 65(||A|| + ||B||)^3.$$

The following estimation holds.

4.5.6 PROPOSITION. Let $A, B, C \in \mathcal{B}_{\mathbb{k}^{n \times n}}(O, \frac{1}{2})$ such that $\exp(A) \exp(B) = \exp(C)$. Then $C = A + B + \frac{1}{2}[A, B] + S$, where the remainder term S satisfies

$$||S|| \le 65 (||A|| + ||B||)^3$$
.

We will derive two main consequences of PROPOSITION 4.5.5 and PROPO-SITION 4.5.6. These relate group operations in $GL(n, \mathbb{k})$ to the linear operations in $\mathbb{k}^{n \times n}$ and are crucial ingredients in the proof that *every matrix group is a Lie group*.

4.5.7 THEOREM. (LIE-TROTTER PRODUCT FORMULA) For $U, V \in \mathbb{k}^{n \times n}$ we have

$$\exp\left(U+V\right) = \lim_{r \to \infty} \left(\exp\left(\frac{1}{r}U\right)\exp\left(\frac{1}{r}V\right)\right)^r.$$

(This formula relates addition in $\mathbb{k}^{n \times n}$ to multiplication in $\mathsf{GL}(n,\mathbb{k})$.)

PROOF : For large r we may take $A = \frac{1}{r}U$ and $B = \frac{1}{r}V$ and apply PROPOSITION 4.5.5 to give

$$\exp\left(\frac{1}{r}U\right)\exp\left(\frac{1}{r}V\right) = \exp\left(C_r\right)$$

with

$$\left\| C_r - \frac{1}{r} (U+V) \right\| \le \frac{17 \left(\|U\| + \|V\| \right)^2}{r^2}.$$

As $r \to \infty$,

$$||rC_r - (U+V)|| \le \frac{17(||U|| + ||V||)^2}{r} \to 0$$

and hence

$$rC_r \to U + V.$$

Since $\exp(rC_r) = \exp(C_r)^r$, the Lie-Trotter product formula follows by continuity of the exponential mapping. \Box

4.5.8 THEOREM. (COMMUTATOR FORMULA) For $U, V \in \mathbb{k}^{n \times n}$ we have

$$\exp([U,V]) = \lim_{r \to \infty} \left(\exp\left(\frac{1}{r}U\right) \exp\left(\frac{1}{r}V\right) \exp\left(-\frac{1}{r}U\right) \exp\left(-\frac{1}{r}V\right) \right)^{r^2}.$$

(This formula relates the Lie bracket - or commutator - in $\mathbb{k}^{n \times n}$ to the group commutator in $GL(n, \mathbb{k})$.)

PROOF: For large r (as in the proof of THEOREM 4.5.7) we have

$$\exp\left(\frac{1}{r}U\right)\exp\left(\frac{1}{r}V\right) = \exp(C_r)$$

with (as $r \to \infty$)

$$rC_r \to U + V.$$

We also have

$$C_r = \frac{1}{r}(U+V) + \frac{1}{2r^2}[U,V] + S_r,$$

where

$$||S_r|| \le 65 \frac{(||U|| + ||V||)^3}{r^3}.$$

Similarly (replacing U, V with -U, -V) we obtain :

$$\exp\left(-\frac{1}{r}U\right)\exp\left(-\frac{1}{r}V\right) = \exp(C_r'),$$

where

$$C'_{r} = -\frac{1}{r}(U+V) + \frac{1}{2r^{2}}[U,V] + S'_{r}$$

and

$$\|S_r'\| \le 65 \frac{(\|U\| + \|V\|)^3}{r^3}.$$

Combining these we get

$$\exp\left(\frac{1}{r}U\right)\exp\left(\frac{1}{r}V\right)\exp\left(-\frac{1}{r}U\right)\exp\left(-\frac{1}{r}V\right) = \exp(C_r)\exp(C'_r)$$
$$= \exp(E_r),$$

where

$$E_r = C_r + C'_r + \frac{1}{2}[C_r, C'_r] + T_r$$

= $\frac{1}{r^2}[U, V] + \frac{1}{2}[C_r, C'_r] + S_r + S'_r + T_r$

 \diamond **Exercise 235** Verify that

$$[C_r, C'_r] = \frac{1}{r^3} [U + V, [U, V]] + \frac{1}{r} [U + V, S_r + S'_r] + \frac{1}{2r^2} [[U, V], S'_r - S_r] + [S_r, S'_r].$$

All four of these terms have norm bounded by an expression of the form $\frac{\text{constant}}{r^3}$ so the same is true of $[C_r, C'_r]$. Also S_r, S'_r, T_r have similarly bounded norms. Setting

$$Q_r := r^2 E_r - [U, V]$$

we obtain (as $r \to \infty$)

$$||Q_r|| = r^2 ||E_r - \frac{1}{r^2}[U, V]|| \le \frac{\text{constant}}{r} \to 0$$

and hence

$$\exp(E_r)^{r^2} = \exp\left([U, V] + Q_r\right) \to \exp([U, V]).$$

The *commutator formula* now follows using continuity of the exponential mapping.

NOTE : If g, h are elements of a group, then the expression $ghg^{-1}h^{-1}$ is called the group commutator of g and h.

There is one further concept involving the exponential mapping that is basic in Lie theory. It involves *conjugation*, which is generally referred to as the "adjoint action". For $g \in \mathsf{GL}(n, \Bbbk)$ and $A \in \Bbbk^{n \times n}$, we can form the conjugate

$$\operatorname{Ad}_q(A) := gAg^{-1}.$$

♦ **Exercise 236** Let $A, B \in \mathbb{k}^{n \times n}$ and $g, h \in \mathsf{GL}(n, \mathbb{k})$. Show that (for $\lambda, \mu \in \mathbb{k}$)

(a)
$$\operatorname{Ad}_g(\lambda A + \mu B) = \lambda \operatorname{Ad}_g(A) + \mu \operatorname{Ad}_g(B).$$

- (b) $\operatorname{Ad}_g([A, B]) = [\operatorname{Ad}_g(A), \operatorname{Ad}_g(B)].$
- (c) $\operatorname{Ad}_{gh}(A) = \operatorname{Ad}_g(\operatorname{Ad}_h(A)).$

In particular, $\operatorname{Ad}_{g}^{-1} = \operatorname{Ad}_{g^{-1}}$.

Formulas (a) an (b) say that Ad_g is an *automorphism* of the Lie algebra $\mathbb{k}^{n \times n}$, and formula (c) says the mapping

$$\operatorname{Ad}:\operatorname{\mathsf{GL}}(n,\Bbbk)\to\operatorname{\mathsf{Aut}}(\Bbbk^{n\times n}),\quad g\mapsto\operatorname{Ad}_g$$

is a group homomorphism. The mapping Ad is called the **adjoint representation** of (the matrix group) GL(n, k).

Formula (c) implies in particular that if $t \mapsto \exp(tA)$ is a one-parameter subgroup of $\mathsf{GL}(n, \Bbbk)$, then $\operatorname{Ad}_{\exp(tA)}$ is a one-parameter group (of linear transformations) in $\Bbbk^{n \times n}$. Observe that we can identify $\operatorname{Aut}(\Bbbk^{n \times n})$ with $\operatorname{GL}(n^2, \Bbbk)$ (and thus view $\operatorname{Aut}(\Bbbk^{n \times n})$ as a matrix group). Then (by THEOREM 4.4.3)

$$\operatorname{Ad}_{\exp(tA)} = \exp(t\mathcal{A})$$

for some $\mathcal{A} \in \mathbb{k}^{n^2 \times n^2} = \mathsf{End}\,(\mathbb{k}^{n \times n})$. Since

$$\mathcal{A}(B) = \left. \frac{d}{dt} \operatorname{Ad}_{\exp(tA)}(B) \right|_{t=0}$$
$$= \left. \frac{d}{dt} \exp(tA) B \exp(-tA) \right|_{t=0}$$
$$= [A, B]$$

by setting (for $A, B \in \mathbb{k}^{n \times n}$)

$$\operatorname{ad} A(B) := [A, B]$$

we have the following formula

$$\operatorname{Ad}_{\exp(tA)} = \exp(t \operatorname{ad} A).$$

Explicitly, the formula says that

$$\exp{(tA)B}\exp{(-tA)} = \sum_{k=0}^{\infty} \frac{t^k}{k!} (\operatorname{ad} A)^k B.$$

(Here $(\operatorname{ad} A)^0 = A$ and $(\operatorname{ad} A)^k = \operatorname{ad}(\operatorname{ad} A)^{k-1}$ for $k \ge 1$.)

NOTE : The mapping

$$\operatorname{ad}: \mathbb{k}^{n \times n} \to \operatorname{End}(\mathbb{k}^{n \times n}), \quad X \mapsto \operatorname{ad} X$$

is called the *adjoint representation* of (the Lie algebra) $\mathbb{k}^{n \times n}$. From the Jacobi identity for Lie algebras, we have

$$\operatorname{ad} X([Y, Z]) = [\operatorname{ad} X(Y), Z] + [Y, \operatorname{ad} X(Z)].$$

That is, ad X is a *derivation* of the Lie algebra $\mathbb{k}^{n \times n}$. The formula above gives the relation between the automorphism $\operatorname{Ad}_{\exp(tX)}$ of the Lie algebra $\mathbb{k}^{n \times n}$ and the derivation ad X of $\mathbb{k}^{n \times n}$. One also has

$$\exp\left(t\mathrm{Ad}_q(X)\right) = g\exp\left(tX\right)g^{-1}.$$

Using this formula, we can see that [X, Y] = 0 if and only if $\exp(tX)$ and $\exp(sY)$ commute for arbitrary $s, t \in \mathbb{R}$.

♦ **Exercise 237** Let $A, B \in \mathbb{k}^{n \times n}$.

(a) Verify that

$$\operatorname{ad}[A, B] = \operatorname{ad} A \operatorname{ad} B - \operatorname{ad} B \operatorname{ad} A = [\operatorname{ad} A, \operatorname{ad} B].$$

(This means that ad : $\mathbb{k}^{n \times n} \to \mathsf{End}(\mathbb{k}^{n \times n})$ is a *Lie algebra homomorphism*.)

(b) Show by induction that

$$(ad A)^n (B) = \sum_{k=0}^n \binom{n}{k} A^k B(-A)^{n-k}.$$

(c) Show by direct computation that

$$\exp\left(\operatorname{ad} A\right)(B) = \operatorname{Ad}_{\exp\left(A\right)}(B) = \exp\left(A\right)B\exp\left(-A\right).$$

4.6 Examples of Lie Algebras of Matrix Groups

The Lie algebras of $GL(n,\mathbb{R})$ and $GL(n,\mathbb{C})$

Let us start with the *real* general linear group $\mathsf{GL}(n,\mathbb{R}) \subseteq \mathbb{R}^{n\times n}$. We have shown (see EXAMPLE 4.4.8) that $T_I\mathsf{GL}(n,\mathbb{R}) = \mathbb{R}^{n\times n}$. Hence the Lie algebra $\mathfrak{gl}(n,\mathbb{R})$ of $\mathsf{GL}(n,\mathbb{R})$ consists of all $n \times n$ matrices (with real entries), with the commutator as the Lie bracket. Thus

$$\mathfrak{gl}(n,\mathbb{R}) = \mathbb{R}^{n \times n}$$

It follows that

$$\dim \mathsf{GL}(n,\mathbb{R}) = \dim \mathfrak{gl}(n,\mathbb{R}) = n^2.$$

Similarly, the Lie algebra of the complex general linear group $\mathsf{GL}(n,\mathbb{C})$ is

$$\mathfrak{gl}(n,\mathbb{C})=\mathbb{C}^{n\times n}$$

and

$$\dim \operatorname{\mathsf{GL}}(n,\mathbb{C}) = \dim_{\mathbb{R}} \mathfrak{gl}(n,\mathbb{C}) = 2n^2.$$

The Lie algebras of $SL(n, \mathbb{R})$ and $SL(n, \mathbb{C})$

For $\mathsf{SL}(n,\mathbb{R}) \leq \mathsf{GL}(n,\mathbb{R})$, suppose that

$$\alpha:(a,b)\to\mathsf{SL}\left(n,\mathbb{R}\right)$$

is a curve in $\mathsf{SL}(n,\mathbb{R})$ with $\alpha(0) = I$. For $t \in (a,b)$ we have det $\alpha(t) = 1$ and so

$$\frac{d}{dt}\det\,\alpha(t) = 0.$$

Using LEMMA 4.5.3, it follows that

$$\operatorname{tr}\dot{\alpha}(0)=0$$

and thus

$$T_I \mathsf{SL}(n, \mathbb{R}) \subseteq \ker \operatorname{tr} := \left\{ A \in \mathbb{R}^{n \times n} \, | \, \operatorname{tr} A = 0 \right\}.$$

If $A \in \ker \operatorname{tr} \subseteq \mathbb{R}^{n \times n}$, the curve

$$\alpha: (a,b) \to \mathbb{R}^{n \times n}, \quad t \mapsto \exp(tA)$$

satisfies (the boundary conditions)

$$\alpha(0) = I$$
 and $\dot{\alpha}(0) = A$.

Moreover, using Liouville's Formula, we get

$$\det \alpha(t) = \det \exp (tA) = e^{t \operatorname{tr} A} = 1.$$

Hence the Lie algebra $\mathfrak{sl}(n,\mathbb{R})$ of $\mathsf{SL}(n,\mathbb{R})$ consists of all $n \times n$ matrices (with real entries) having trace zero, with the commutator as the Lie bracket. Thus

$$\mathfrak{sl}(n,\mathbb{R}) = T_I \mathsf{SL}(n,\mathbb{R}) = \{A \in \mathfrak{gl}(n,\mathbb{R}) \mid \mathrm{tr} A = 0\}.$$

Since $\operatorname{tr} A = 0$ imposes one condition on A, it follows that

$$\dim \mathsf{SL}(n,\mathbb{R}) = \dim_{\mathbb{R}} \mathfrak{sl}(n,\mathbb{R}) = n^2 - 1.$$

Similarly, the Lie algebra of the complex special linear group $SL(n, \mathbb{C})$ is

$$\mathfrak{sl}(n,\mathbb{C}) = T_I \mathsf{SL}(n,\mathbb{C}) = \{A \in \mathfrak{gl}(n,\mathbb{C}) \mid \operatorname{tr} A = 0\}$$

and

$$\dim \mathsf{SL}(n,\mathbb{C}) = \dim_{\mathbb{R}} \mathfrak{sl}(n,\mathbb{C}) = 2(n^2 - 1).$$

The Lie algebras of O(n) and SO(n)

First, consider the orthogonal group O(n); that is,

$$\mathsf{O}(n) = \left\{ A \in \mathsf{GL}(n, \mathbb{R}) \, | \, A^{\top} A = I \right\} \le \mathsf{GL}(n, \mathbb{R}).$$

Given a curve $\alpha : (a, b) \to \mathsf{O}(n)$ with $\alpha(0) = I$, we have

$$\frac{d}{dt}\alpha(t)^T\alpha(t)=0$$

and so

$$\dot{\alpha}(t)^T \alpha(t) + \alpha(t)^T \dot{\alpha}(t) = 0$$

which implies

$$\dot{\alpha}(0)^T + \dot{\alpha}(0) = 0$$

Thus we must have $\dot{\alpha}(0) \in \mathbb{R}^{n \times n}$ is *skew-symmetric*. So

$$T_{I}\mathsf{O}(n) \subseteq \mathsf{Sk-sym}(n) = \left\{ A \in \mathbb{R}^{n \times n} \, | \, A^{\top} + A = 0 \right\}$$

(the set of all $n \times n$ skew-symmetric matrices in $\mathbb{R}^{n \times n}$).

On the other hand, if $A \in \mathsf{Sk-sym}(n) \subseteq \mathbb{R}^{n \times n}$, we consider the curve

$$\alpha: (a,b) \to \mathsf{GL}(n,\mathbb{R}), \quad t \mapsto \exp(tA).$$

Then

$$\alpha(t)^{\top} \alpha(t) = \exp(tA)^{\top} \exp(tA)$$
$$= \exp(tA^{\top}) \exp(tA)$$
$$= \exp(-tA) \exp(tA)$$
$$= I.$$

Hence we can view α as a curve in O(n). Since $\dot{\alpha}(0) = A$, this shows that

$$\mathsf{Sk-sym}(n) \subseteq T_I \mathsf{O}(n)$$

and hence the Lie algebra $\mathfrak{o}(n)$ of the orthogonal group O(n) consists of all $n \times n$ skew-symmetric matrices, with the usual commutator as the Lie bracket. Thus

$$\mathfrak{o}(n) = T_I \mathsf{O}(n) = \mathsf{Sk-sym}(n) = \left\{ A \in \mathbb{R}^{n \times n} \, | \, A^\top + A = 0 \right\}.$$

It follows that (see PROPOSITION 4.4.9)

$$\dim \mathsf{O}(n) = \dim \mathfrak{o}(n) = \frac{n(n-1)}{2}$$

♦ **Exercise 238** Show that if $A \in Sk-sym(n)$, then tr A = 0.

By Liouville's Formula, we have

$$\det \alpha(t) = \det \exp \left(tA\right) = 1$$

and hence $\alpha : (a, b) \to SO(n)$, where SO(n) is the special orthogonal group. We have actually shown that the Lie algebra of the special orthogonal group SO(n) is

$$\mathfrak{so}(n) = \mathfrak{o}(n) = \left\{ A \in \mathbb{R}^{n \times n} \, | \, A^{\top} + A = 0 \right\}.$$

The Lie algebra of SO(3)

We will discuss the Lie algebra $\mathfrak{so}(3)$ of the rotation group $\mathsf{SO}(3)$ in some detail.

 $\diamond~Exercise~239~$ Show that

$$\mathfrak{so}(3) = \left\{ \begin{bmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{bmatrix} \in \mathbb{R}^{3 \times 3} \mid a, b, c \in \mathbb{R} \right\}.$$

The Lie algebra $\mathfrak{so}(3)$ is a 3-dimensional real vector space. Consider the rotations

$$R_1(t) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{bmatrix}, R_2(t) = \begin{bmatrix} \cos t & 0 & \sin t \\ 0 & 1 & 0 \\ -\sin t & 0 & \cos t \end{bmatrix}, R_3 = \begin{bmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then the mappings

$$\rho_i: t \mapsto R_i(t), \quad i = 1, 2, 3$$

are curves in SO(3) and clearly $\rho_i(0) = I$. It follows that

$$\dot{\rho}_i(0) := A_i \in \mathfrak{so}(3), \quad i = 1, 2, 3.$$

These elements (matrices) are

$$A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

 \diamond **Exercise 240** Verify that the matrices A_1, A_2, A_3 form a basis for $\mathfrak{so}(3)$. We shall refer to this basis as the *standard basis*.

 \diamond **Exercise 241** Compute all the Lie brackets (commutators) $[A_i, A_j]$, i, j = 1, 2, 3 and then determine the coefficients c_{ij}^k defined by

$$[A_i, A_j] = c_{ij}^1 A_1 + c_{ij}^2 A_2 + c_{ij}^3 A_3, \quad i, j = 1, 2, 3.$$

These coefficients are called the *structure constants* of the Lie algebra. They determine completely the Lie bracket $[\cdot, \cdot]$.

The Lie algebra $\mathfrak{so}(3)$ may be *identified* with (the Lie algebra) \mathbb{R}^3 as follows. We define the mapping

$$\widehat{}: \mathbb{R}^3 \to \mathfrak{so}(3), \quad x = (x_1, x_2, x_3) \mapsto \widehat{x} := \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix}.$$

This mapping is called the *hat mapping*.

♦ **Exercise 242** Show that the hat mapping $\widehat{}: \mathbb{R}^3 \to \mathfrak{so}(3)$ is an *isomorphism* of vector spaces.

- ♦ **Exercise 243** Show that (for $x, y \in \mathbb{R}^3$)
 - (a) $x \times y = \hat{x} y$. (b) $\widehat{x \times y} = [\hat{x}, \hat{y}]$. (c) $x \bullet y = -\frac{1}{2} \operatorname{tr} (\hat{x} \hat{y})$.

Formula (b) says that the hat mapping is in fact an isomorphism of Lie algebras and so we can identify the Lie algebra $\mathfrak{so}(3)$ with (the Lie algebra) \mathbb{R}^3 .

NOTE: For $x \in \mathbb{R}^3$ and $t \in \mathbb{R}$, the matrix exponential $\exp(t \hat{x})$ is a *rotation* about (the axis) x through the angle t||x||. The following explicit formula for $\exp(\hat{x})$ is known as *Rodrigues' Formula*:

$$\exp\left(\widehat{x}\right) = I + \frac{\sin\left\|x\right\|}{\|x\|}\,\widehat{x} + \frac{1}{2}\left[\frac{\sin\left(\frac{\|x\|}{2}\right)}{\frac{\|x\|}{2}}\right]^2\,\widehat{x}^2.$$

This result says that the exponential mapping

$$\exp:\mathfrak{so}(3)\to\mathsf{SO}(3)$$

is onto. Rodrigues' Formula is useful in *computational solid mechanics*, along with its quaternionic counterpart.

The Lie algebras of U(n) and SU(n)

Consider the unitary group U(n); that is,

$$\mathsf{U}(n) = \{A \in \mathsf{GL}(n, \mathbb{C}) \,|\, A^*A = I\}.$$

For a curve α in U(n) with $\alpha(0) = I$, we obtain

$$\dot{\alpha}(0)^* + \dot{\alpha}(0) = 0$$

and so $\dot{\alpha}(0) \in \mathbb{C}^{n \times n}$ is skew-Hermitian. So

$$T_{I}\mathsf{U}(n) \subseteq \mathsf{Sk-Herm}(n) = \{A \in \mathbb{C}^{n \times n} | A^{*} + A = 0\}$$

(the set of all $n \times n$ skew-Hermitian matrices in $\mathbb{C}^{n \times n}$).

If $H \in \mathsf{Sk-Herm}(n)$, then the curve

$$\alpha: (a,b) \to \mathsf{GL}(n,\mathbb{C}), \quad t \mapsto \exp(tH)$$

satisfies

$$\alpha(t)^* \alpha(t) = \exp(tH)^* \exp(tH)$$

= $\exp(tH^*) \exp(tH)$
= $\exp(-tH) \exp(tH)$
= $I.$

Hence we can view α as a curve in U(n). Since $\dot{\alpha}(0) = H$, this shows that

Sk-Herm
$$(n) \subseteq T_I U(n)$$

and hence the Lie algebra $\mathfrak{u}(n)$ of the unitary group $\mathsf{U}(n)$ consists of all $n \times n$ skew-Hermitian matrices, with the usual commutator as the Lie bracket. Thus

$$\mathfrak{u}(n) = T_I \mathsf{U}(n) = \mathsf{Sk-Herm}(n) = \left\{ H \in \mathbb{C}^{n \times n} \, | \, H^* + H = 0 \right\}.$$

It follows that (see Exercise 229)

$$\dim \mathsf{U}(n) = \dim_{\mathbb{R}} \mathfrak{u}(n) = n^2.$$

The special unitary group $\mathsf{SU}(n)$ can be handled in a similar way. Again we have

$$\mathfrak{su}(n) = T_I \mathsf{SU}(n) \subseteq \mathsf{Sk-Herm}(n).$$

But also if $\alpha : (a,b) \to \mathsf{SU}(n)$ is a curve with $\alpha(0) = I$ then, as in the analysis for $\mathsf{SL}(n,\mathbb{R})$,

$$\operatorname{tr} \dot{\alpha}(0) = 0.$$

Writing

$$\mathsf{Sk-Herm}^{0}(n) := \{ H \in \mathsf{Sk-Herm}(n) \, | \, \mathrm{tr} \, H = 0 \}$$

this gives $\mathfrak{su}(n) \subseteq \mathsf{Sk-Herm}^0(n)$. On the other hand, if $H \in \mathsf{Sk-Herm}^0(n)$ then the curve

$$\alpha: (a, b) \to \mathsf{U}(n), \quad t \mapsto \exp(tH)$$

takes values in SU(n) and $\dot{\alpha}(0) = H$. Hence

$$\mathfrak{su}(n) = T_I \mathsf{SU}(n) = \mathsf{Sk-Herm}^0(n) = \left\{ H \in \mathbb{C}^{n \times n} \, | \, H^* + H = 0 \text{ and } \operatorname{tr} H = 0 \right\}.$$

NOTE : For a matrix group $G \leq \mathsf{GL}(n, \mathbb{R})$ (with Lie algebra \mathfrak{g}), the following are true (and can be used in determining Lie algebras of matrix groups).

• The mapping

$$\exp_G : \mathfrak{g} \to \mathsf{GL}(n,\mathbb{R}), \quad X \mapsto \exp(X)$$

has image contained in G, $\exp_G(\mathfrak{g}) \subseteq G$. We will normally write $\exp_G : \mathfrak{g} \to G$ for the exponential mapping on G (and sometimes even just exp). In general, the exponential mapping \exp_G is neither one-to-one nor onto.

- If G is compact and connected, then \exp_G is onto.
- The mapping \exp_G maps a neighborhood of 0 in \mathfrak{g} bijectively onto a neighborhood of I in G.
- ♦ Exercise 244 Verify that the exponential mapping

$$\exp_{\bigcup(1)} : \mathbb{R} \to \bigcup(1) = \mathbb{S}^1, \quad t \mapsto e^{it}$$

is onto but not one-to-one.
4.6.1 EXAMPLE. The exponential mapping

$$\exp_{\mathsf{SL}(2,\mathbb{R})}:\mathfrak{sl}(2,\mathbb{R})\to\mathsf{SL}(2,\mathbb{R})$$

is not onto. Let

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{bmatrix} \quad \text{with } \lambda < -1.$$

We see that $A \in \mathsf{SL}(2,\mathbb{R})$ and we shall show that A is *not* of the form $\exp(X)$ with $X \in \mathfrak{sl}(2,\mathbb{R})$. If $A = \exp(X)$, then the eigenvalues of A are of the form e^a and e^b , where a and b are the eigenvalues of X. Suppose $\lambda = e^a$ and $\frac{1}{\lambda} = e^b$. Then

$$a = -b + 2k\pi i, \quad k \in \mathbb{Z}.$$

However, since λ is negative, a is actually complex and therefore its conjugate is also an eigenvalue; that is, $b = \bar{a}$. This gives a as pure imaginary. Then

$$1 = |e^a| = |\lambda| = -\lambda$$

which contradicts the assumption that $\lambda < -1$.

The Lie algebra of SU(2)

We will discuss the Lie algebra $\mathfrak{su}(2)$ in some detail.

 \diamond Exercise 245 Show that

$$\mathfrak{su}(2) = \left\{ \begin{bmatrix} ci & -b + ai \\ b + ai & -ci \end{bmatrix} \in \mathbb{C}^{2 \times 2} \, | \, a, b, c \in \mathbb{R} \right\}.$$

The Lie algebra $\mathfrak{su}(2)$ is a 3-dimensional real vector space. Consider the matrices

$$H_1 = \frac{1}{2} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad H_2 = \frac{1}{2} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad H_3 = \frac{1}{2} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

Clearly,

$$H_i \in \mathfrak{su}(2), \quad i = 1, 2, 3.$$

 \diamond **Exercise 246** Verify that the matrices H_1, H_2, H_3 form a basis for $\mathfrak{su}(2)$.

♦ **Exercise 247** Compute all the Lie brackets (commutators) $[H_i, H_j]$, i, j = 1, 2, 3 and then determine the structure constants of (the Lie algebra) $\mathfrak{su}(2)$.

Consider the mapping

$$\phi : \mathbb{R}^3 \to \mathfrak{su}(2), \quad x = (x_1, x_2, x_3) \mapsto x_1 H_1 + x_2 H_2 + x_3 H_3.$$

♦ **Exercise 248** Show that the mapping $\phi : \mathbb{R}^3 \to \mathfrak{su}(2)$ is an *isomorphism* of Lie algebras.

Thus we can identify the Lie algebra $\mathfrak{su}(2)$ with (the Lie algebra) \mathbb{R}^3 .

NOTE : The Lie algebras $\mathfrak{su}(2)$ and $\mathfrak{so}(3)$ look the same algebraically (they are isomorphic). An explicit isomorphism (of Lie algebras) is given by

$$\psi: x_1H_1 + x_2H_2 + x_3H_3 \mapsto x_1A_1 + x_2A_2 + x_3A_3.$$

This suggests that there might be a close relationship between the matrix groups themselves. Indeed there is a (surjective) *Lie homomorphism* $SU(2) \rightarrow SO(3)$ whose derivative (at I) is ψ . Recall the adjoint representation

$$\operatorname{Ad}: \operatorname{\mathsf{SU}}(2) \to \operatorname{\mathsf{Aut}}(\mathfrak{su}(2)), \quad A \mapsto \operatorname{Ad}_A(: U \mapsto AUA^*).$$

Each Ad_A is a *linear isomorphism* of $\mathfrak{su}(2)$. Ad_A is actually an *orthogonal transfor*mation on $\mathfrak{su}(2)$ (the mapping $(X, Y) \mapsto -\operatorname{tr}(XY)$ is an inner product on $\mathfrak{su}(2)$) and so Ad_A corresponds to an element of O(3) (in fact, SO(3)). The mapping

$$\overline{\mathrm{Ad}}$$
: SU (2) \rightarrow SO (3), $A \mapsto \mathrm{Ad}_A$

turns out to be a continuous homomorphism of matrix groups that is differentiable (i.e., a Lie homomorphism) and such that its derivative $d \operatorname{Ad} : \mathfrak{su}(2) \to \mathfrak{so}(3)$ is ψ .

The Lie algebras of UT(n, k) and $UT^{u}(n, k)$

Let $\alpha : (a, b) \to \mathsf{UT}(n, \Bbbk)$ be a curve in $\mathsf{UT}(n, \Bbbk)$ with $\alpha(0) = I$. Then $\dot{\alpha}(0)$ is upper triangular. Moreover, using the argument for $\mathsf{GL}(n, \Bbbk)$ we see that given any upper triangular matrix $A \in \Bbbk^{n \times n}$, there is a curve

$$\sigma: (-\epsilon, \epsilon) \to \mathbb{k}^{n \times n}, \quad t \mapsto tA + I$$

such that $\sigma(t) \in UT(n, \mathbb{k})$ and $\dot{\sigma}(0) = A$. Hence the Lie algebra $\mathfrak{ut}(n, \mathbb{k})$ of $UT(n, \mathbb{k})$ consists of all $n \times n$ upper triangular matrices, with the usual commutator as the Lie bracket. Thus

$$\mathfrak{ut}(n,\mathbb{k}) = T_I \mathsf{UT}(n,\mathbb{k}) = \left\{ A \in \mathbb{k}^{n \times n} \, | \, a_{ij} = 0 \, \text{ for } i > j \right\}.$$

It follows that

$$\dim \mathsf{UT}(n, \Bbbk) = \dim_{\mathbb{R}} \mathfrak{ut}(n, \Bbbk) = \frac{n(n+1)}{2} \dim_{\mathbb{R}} \Bbbk.$$

An upper triangular matrix $A \in \mathbb{k}^{n \times n}$ is strictly upper triangular if all its diagonal entries are 0. Then the Lie algebra of the unipotent group $UT^u(n, \mathbb{k})$ consists of all $n \times n$ strictly upper triangular matrices, with the usual commutator as the Lie bracket. So

$$\mathfrak{sut}(n, \mathbb{k}) = T_I \mathsf{UT}^u(n, \mathbb{k}) = \left\{ A \in \mathbb{k}^{n \times n} \, | \, a_{ij} = 0 \ \text{ for } i \ge j \right\}.$$

♦ **Exercise 249** Find dim_{\mathbb{R}} sut (n, \mathbb{k}) .

 \diamond **Exercise 250** For each of the following matrix group *G*, determine its Lie algebra \mathfrak{g} and hence its dimension.

(a)
$$G = \{A \in \mathsf{GL}(2,\mathbb{R}) | AQA^{\top} = Q\}$$
, where $Q = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
(b) $G = \{A \in \mathsf{GL}(2,\mathbb{R}) | AQA^{\top} = Q\}$, where $Q = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
(c) $G = \mathsf{GA}(3,\mathbb{R})$.

- (d) G =Heis.
- (e) $G = G_4 \leq \mathsf{UT}^u(4,\mathbb{R})$ from **Exercise 199**.
- (f) $G = \mathsf{E}(n)$.
- (g) $G = \mathsf{SE}(n)$.

♦ Exercise 251

(a) Show that the Lie algebra of the symplectic group $\mathsf{Sp}(2n,\mathbb{R})$ is

$$\mathfrak{sp}(2n,\mathbb{R}) = \left\{ A \in \mathbb{R}^{2n \times 2n} \, | \, A^{\top} \mathbb{J} + \mathbb{J}A = 0 \right\}.$$

(b) If

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathfrak{sl}(2n, \mathbb{R})$$

show that $A \in \mathfrak{sp}(2n, \mathbb{R})$ if and only if

$$d = -a^{\top}, \quad c = c^{\top}, \quad \text{and} \quad b = b^{\top}.$$

(c) Calculate the dimension of $\mathfrak{sp}(2n,\mathbb{R})$.

 $\diamond~Exercise~252$ Show that the Lie algebra of the Lorentz group \mbox{Lor} is

$$\mathfrak{lor} = \left\{ A \in \mathbb{R}^{4 \times 4} \, | \, SA + A^{\top}S = 0 \right\} = \left\{ \begin{bmatrix} 0 & a_1 & a_2 & a_3 \\ -a_1 & 0 & a_4 & a_5 \\ -a_2 & -a_4 & 0 & a_6 \\ a_3 & a_5 & a_6 & 0 \end{bmatrix} \, | \, a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{R} \right\}$$

♦ **Exercise 253** Consider the matrix group $\Bbbk^{\times} = \mathsf{GL}(1, \Bbbk)$. (Its Lie algebra is clearly \Bbbk .)

(a) Show that the *determinant* function

$$\det:\mathsf{GL}\left(n,\Bbbk\right)\to\Bbbk^{\times}$$

is a *Lie homomorphism* (i.e. a continuous homomorphism of matrix groups that is also *differentiable*; cf. DEFINITION 4.4.14).

(b) Show that the induced *homomorphism* of Lie algebras (i.e. the derivative of det) is the *trace* function

$$\mathrm{tr}: \mathbb{k}^{n \times n} \to \mathbb{k}.$$

(c) Derive from (b) that (for $A, B \in \mathbb{k}^{n \times n}$)

$$\operatorname{tr}(AB) = \operatorname{tr}(BA).$$