1

The exponential map

1.1 Vector fields and one-parameter groups of linear transformations[1]

A linear transformation X of the n-dimensional real or complex vector space E can be thought of as a vector field: X associates to each point p in E, the vector $X(p)$. As an aid to one's imagination one may think of a fluid in motion, so that the velocity of the fluid particles passing through the point p is always $X(p)$; the vector field is then the *current* of the flow and the paths of the fluid particles are the *trajectories*. Of course, this type of flow is very special, in that the current $X(p)$ at p is independent of time (*stationary*) and depends linearly on p. Figure 1 shows the trajectories of such flows in the plane. (We shall see later, that in appropriate linear coordinates every plane flow corresponds to exactly one of these pictures.)

Consider the trajectory of the fluid particle that passes a certain point p_0 at time $\tau = \tau_0$. If $p(\tau)$ is its position at time τ, then its velocity at this time is $p'(\tau) = dp(\tau)/d\tau$. Since the current at $p(\tau)$ is supposed to be $X(p(\tau))$, one finds that $p(\tau)$ satisfies the differential equation

$$p'(\tau) = X(p(\tau)) \tag{1}$$

together with the initial condition

$$p(0) = p_0. \tag{2}$$

The solution of (1) and (2) may be obtained as follows. Try for $p(\tau)$ a power series in τ:

$$p(\tau) = \sum_{k=0}^{\infty} \tau^k p_k$$

[1] Refer to the appendix to §1.1 for an explanation of the notation as necessary.

with coefficients $p_k \in E$ to be determined. Ignoring convergence question for the moment, eqn (1) becomes

$$\sum_{k=1}^{\infty} k\tau^{k-1} p_k = \sum_{k=0}^{\infty} \tau^k X^k(p_k),$$

which leads to

$$p_{k+1} = \frac{1}{k+1} X(p_k).$$

These equations determine p_k inductively in terms of p_0:

$$p_k = \frac{1}{k!} X(p_0).$$

We write the solution $p(\tau)$ thus found in the form

$$p(\tau) = \exp(\tau X) p_0, \tag{3}$$

where the *exponential* of a matrix X is defined by

$$\exp X = \sum_{k=0}^{\infty} \frac{1}{k!} X^k.$$

This exponential function is a fundamental concept, which underlies just about everything to follow. First of all, the exponential series converges in norm for all matrices X, and (3) represents a genuine solution of (1) and (2). (See the appendix to this section.) We shall see momentarily that it is in fact the *only* differentiable solution, but first we shall prove some basic properties of the matrix exponential:

Proposition 1.
(a) For any matrix X,

$$\frac{d}{d\tau} \exp \tau X = X \exp(\tau X) = \exp(\tau X) X,$$

and $a(\tau) = \exp \tau X$ is the unique differentiable solution of

$$a'(\tau) = X a(\tau), \quad a(0) = 1$$

(and also of $a'(\tau) = a(\tau) X, a(0) = 1$).
(b) For any two commuting matrices X, Y,

$$\exp X \exp Y = \exp(X + Y).$$

(c) $\exp X$ is invertible for any matrix X and

$$(\exp X)^{-1} = \exp(-X).$$

(d) For any matrix X and scalars σ, τ

$$\exp(\sigma + \tau) X = \exp(\sigma X) \exp(\tau X),$$

and $a(\tau) = \exp \tau X$ is the unique differentiable solution of $a(\sigma + \tau) = a(\sigma) a(\tau)$, $a(0) = 1$, $a'(0) = X$.

Proof.
(a) Because of the norm-convergence of the power series for $\exp \tau X$ (appendix), we can differentiate it term-by-term:

$$\frac{d}{d\tau}(\exp \tau X) = \frac{d}{d\tau} \sum_{j=0}^{\infty} \frac{\tau^j}{j!} X^j = \sum_{j=1}^{\infty} \frac{\tau^{j-1}}{(j-1)!} X^j,$$

and this is $X \exp(\tau X) = \exp(\tau X) X$, as one sees by factoring out X from this series, either to the left or to the right.

To prove the second assertion of (a), assume $a(\tau)$ satisfies

$$a'(\tau) = X(a(\tau)), \quad a(0) = 1.$$

Differentiating according to the rule $(ab)' = a'b + ab'$ (appendix) we get

$$\begin{aligned} \frac{d}{d\tau}(\exp(-\tau X) a(\tau)) &= \left(\frac{d}{d\tau} \exp -\tau X\right) a(\tau) + \exp(-\tau X) \left(\frac{d}{d\tau} a(\tau)\right) \\ &= \exp(-\tau X)(-X) a(\tau) + \exp(-\tau X) X a(\tau) = 0. \end{aligned}$$

So $\exp(-\tau X) a(\tau)$ is independent of τ, and equals 1 for $\tau = 0$, hence it equals 1 identically. The assertion will now follow from (c).

(b) As for scalar series, the product of two norm-convergent matrix series can be computed by forming all possible products of terms of the first series with terms of the second and then summing in any order. If we apply this recipe to $\exp X \exp Y$, we get,

$$\exp X \exp Y = \left(\sum_{j=0}^{\infty} \frac{X^j}{j!}\right) \left(\sum_{k=0}^{\infty} \frac{Y^k}{k!}\right) = \sum_{j,k=0}^{\infty} \frac{X^j Y^k}{j!k!}. \tag{4}$$

On the other hand, *assuming* X and Y *commute*, we can rearrange and collect terms while expanding $(1/m!)(X+Y)^m$ to get

$$\exp(X+Y) = \sum_{m=0}^{\infty} \frac{1}{m!}(X+Y)^m = \sum_{m=0}^{\infty} \frac{1}{m!} \left(\sum_{j+k=m} \frac{m!}{j!k!} X^j Y^k\right) = \sum_{j,k=0}^{\infty} \frac{X^j Y^k}{j!k!}. \tag{5}$$

Comparison of (4) and (5) gives (b).

(c) This follows from (b) with $Y = -X$.

(d) The first assertion comes from (b) with X replaced by σX and Y by τX. To prove the second assertion, assume $a(\tau)$ has the indicated property. Then

$$a'(\tau) = \frac{d}{d\sigma} a(\tau + \sigma)\bigg|_{\sigma=0} = a(\tau) \frac{d}{d\sigma} a(\sigma)\bigg|_{\sigma=0} = a(\tau) X, \tag{6}$$

and the assertion follows from the second part of (a). QED

Remark 2. For (b) it is essential that X and Y commute. In fact, the following statements are equivalent:

(a) X and Y commute.

(b) $\exp \sigma X$ and $\exp \tau Y$ commute for all scalars σ, τ.

(c) $\exp(\sigma X + \tau Y) = \exp(\sigma X) \exp(\tau Y)$ for all scalars σ, τ. (QED)

It is now easy to see that $p'(\tau) = X(p(\tau))$ and $p(0) = p_0$ implies $p(\tau) = \exp(\tau X)p_0$: that $p(\tau) = \exp(\tau X)p_0$ satisfies $p'(\tau) = X(p(\tau))$ and $p(0) = p_0$ is clear from part (a) of the proposition; and the uniqueness of this solution is seen by differentiating $\exp(-\tau X)p(\tau)$ as in the proof of the uniqueness of (a).

The properties of the matrix exponential summarized in the proposition are of basic importance. Parts (c) and (d) may be rephrased by saying that, for fixed X, the map $\tau \to \exp \tau X$ is a *homomorphism* of the group of scalars under addition ($\mathbb{R}$ or $\mathbb{C}$) into the *general linear group* $\mathrm{GL}(E)$ of all invertible linear transformations of E. This map $\tau \to \exp \tau X$ is called the *one-parameter group generated by* X, even though it is a group homomorphism rather than a group.

The group property $\exp(\sigma X) \exp(\tau X) = \exp(\sigma + \tau)X$ of exp is intimately related to the stationary property of flow in the physical picture: it may be interpreted as saying that two fluid particles passing through the same point at different times will travel along the same path, passing through the same points, after equal time intervals.

There is another simple property of exp that is frequently used:

Proposition 3. *For any matrix X and any invertible matrix a,*

$$a(\exp X)a^{-1} = \exp(aXa^{-1}).$$

Proof.

$$a \exp(X)a^{-1} = a\left(\sum_{k=0}^{\infty} \frac{X^k}{k!}\right)a^{-1} = \sum_{k=0}^{\infty} \frac{(aXa^{-1})^k}{k!} = \exp(aXa^{-1}).$$

QED

Incidentally, the property of exp expressed by the proposition is shared by any convergent matrix-power series. It only relies on the fact that the *conjugation* operation $X \to aXa^{-1}$ in the matrix space $M = L(E)$ is linear and preserves product of matrices:

$$a(\alpha X + \beta Y)a^{-1} = \alpha(aXa^{-1}) + \beta(aYa^{-1}),$$
$$a(XY)a^{-1} = (aXa^{-1})(aYa^{-1}).$$

Proposition 3 is often useful for computing matrix exponentials. For example, if X is diagonalizable, then $X = aYa^{-1}$, where Y is the diagonal, and $\exp X = a(\exp Y)a^{-1}$. The exponential of a diagonal matrix is easy to compute:

$$\exp \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} = \sum_{k=0}^{\infty} \frac{1}{k!} \begin{bmatrix} \lambda_1^k & & \\ & \ddots & \\ & & \lambda_n^k \end{bmatrix} = \begin{bmatrix} e^{\lambda_1} & & \\ & \ddots & \\ & & e^{\lambda_n} \end{bmatrix}.$$

Example 4 (Exponential of 2×2 matrices).

(i) Every real 2×2 matrix is conjugate to exactly one of the following types with $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$.

(a) *Elliptic:* $\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. (b) *Hyperbolic:* $\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

(c) *Parabolic:* $\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$. (d) *Scalar:* $\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(ii) The matrices X given above in (a)–(d) generate the following one-parameter groups $\exp \tau X$.

(a) *Elliptic:* $e^{\alpha\tau} \begin{bmatrix} \cos \beta\tau & -\sin \beta\tau \\ \sin \beta\tau & \cos \beta\tau \end{bmatrix}$. (b) *Hyperbolic:* $e^{\alpha\tau} \begin{bmatrix} \cosh \beta\tau & \sinh \beta\tau \\ \sinh \beta\tau & \cosh \beta\tau \end{bmatrix}$.

(c) *Parabolic:* $e^{\alpha\tau} \begin{bmatrix} 1 & 0 \\ \beta\tau & 1 \end{bmatrix}$. (d) *Scalar:* $e^{\alpha\tau} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

The normal forms in (i) may be derived by manipulating with eigenvalues and eigenvectors, which we omit. As a sample calculation with exp, we verify the formulas in (ii).

(a)

$$\exp\left(\alpha\tau \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta\tau \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) = \exp\left(\alpha\tau \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \exp\left(\beta\tau \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right)$$

because the matrices commute. The first factor is $e^{\alpha\tau} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

To evaluate the second one, note that

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^{2k} = (-1)^k \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^{2k+1} = (-1)^k \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Therefore,

$$\exp\left(\tau\beta \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) = \sum_{k=0}^{\infty} \frac{(-1)^k (\tau\beta)^{2k}}{(2k)!} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \sum_{k=0}^{\infty} \frac{(-1)^k (\tau\beta)^{2k+1}}{(2k+1!)} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Recognizing the sin and cos series one gets (a).

Comment. The exponential just calculated may also be found by diagonalization:

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}^{-1} \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}.$$

(b) This is similar.

(c) In this case, one actually gets a finite sum for exp of the second (non-scalar) summand in part (c) of (i):

$$\exp \tau \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \tau \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

This kind of thing will evidently, always happen if one takes the exponential of a nilpotent matrix, i.e. a matrix X for which $X^k = 0$ for some k.

Using the formulas in (ii) one may verify that the pictures in Figure 1 correspond to the normal forms of the vector fields in (i).

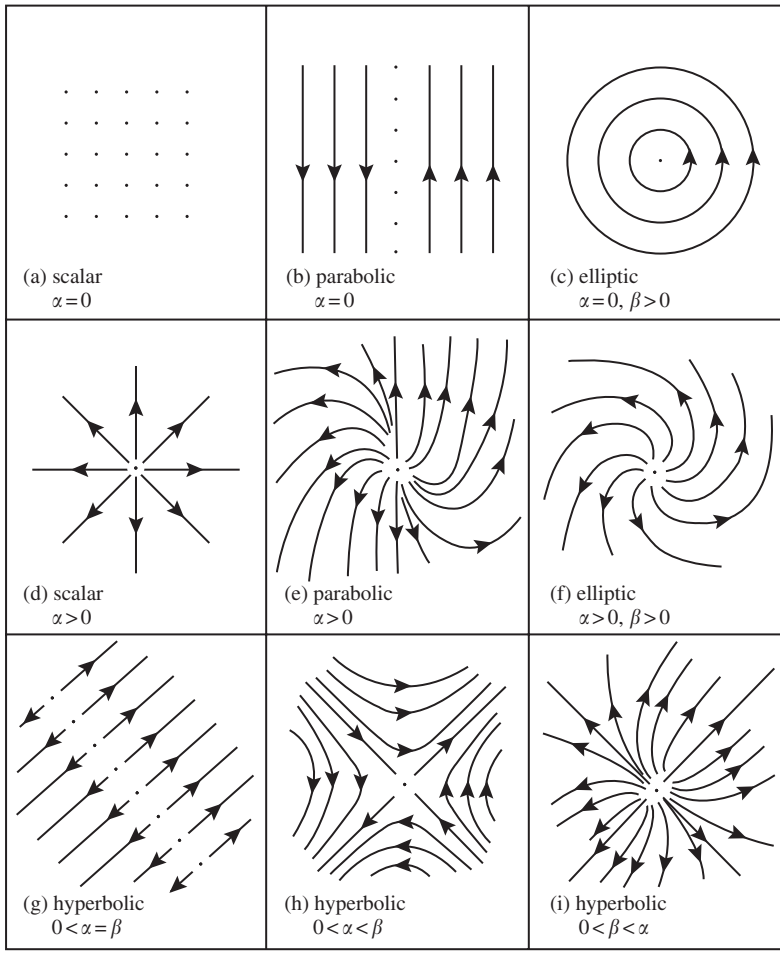

Fig. 1

Problems for §1.1

1. Prove Remark 2.

2. Verify the formula for exponential in the hyperbolic case given in Example 4: (a) by power series calculation, (b) by diagonalization.

3. Show that $\exp \tau X$ is orthogonal (unitary) for all $\tau \in \mathbb{R}$ if and only if X is skew-symmetric (skew-Hermitian).

4. Let $E = \mathbb{R}^3$, $0 \neq x \in E$, X be the linear transformation of $p \to (x \times p)$ of E (cross-product).

   (a) Choose a right-handed orthonormal basis (e_1, e_2, e_3) for E *with* e_3 a unit vector parallel to x. Show that

   $$\begin{aligned} \exp(X)e_1 &= \cos\|x\|e_1 + \sin\|x\|e_2, \\ \exp(X)e_2 &= -\sin\|x\|e_1 + \cos\|x\|e_2, \\ \exp(X)e_3 &= e_3. \end{aligned}$$

   [For the purpose of this problem, an ordered orthonormal basis (e_1, e_2, e_3) for E may be defined to be *right-handed*, if it satisfies the usual cross-product relation given by the 'right-hand rule', i.e.

   $$e_1 \times e_2 = e_3, \quad e_2 \times e_3 = e_1, \quad e_3 \times e_1 = e_2.$$

   Any orthonormal basis can be ordered so that it becomes right–handed. The above formula means that $\exp(X)$ is the right-handed rotation around x with an angle $\|x\|$.]

   (b) Show that

   $$\exp(X) = 1 + \frac{\sin\|x\|}{\|x\|}(X) + \frac{1 - \cos\|x\|}{\|x\|^2}(X)^2.$$

5. Show:

   $$\exp \begin{bmatrix} \lambda & 1 & 0 \cdots & 0 \\ 0 & \lambda & 1 \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \cdots & \lambda \end{bmatrix} = \begin{bmatrix} e^\lambda & e^\lambda & e^\lambda/2! \cdots & e^\lambda/(n-1)! \\ 0 & e^\lambda & e^\lambda \cdots & e^\lambda/(n-2)! \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \cdots & e^\lambda \end{bmatrix}.$$

6. Let E be the space of all polynomials $f(\xi) = c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}$ of degree $\leq (n-1)$ (some fixed n; the coefficients c_j can be taken either real or complex). The derivative $Df(\xi) = f'(\xi)$ defines a linear transformation D of E. Show:

   $$\exp(\tau D)f(\xi) = f(\xi + \tau).$$

   This problem is related to the previous one. Explain how.

7. Show that
$$\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$
is not the exponential of any real 2×2 matrix. [Suggestion: consider eigenvalues and eigenvectors.]

8. An *affine transformation* of E is a transformation of the form $p \to ap + b$ where $a \in M$ is linear and $b \in E$ operates as a translation $p \to p + b$. An affine transformation may again be interpreted as a vector field on E, called *affine vector field*, typically denoted by $p \to Xp + v$ where $X \in M$ and $v \in E$.

   Think of E as embedded on the hyperplane $E^+ = \{(p, 1)\}$ in a space $E \times \mathbb{R}$ (or $E \times \mathbb{C}$) of one higher dimension by identifying $p \in E$ with $p^+ = (p, 1) \in E^+$. The vectors of $E \times \mathbb{R}$ (or $E \times \mathbb{C}$) tangential to E^+ are those of the form $(y, 0)$ [*not* $(y, 1)$] and a vector field on E^+ associates to each point $(p, 1)$ such a vector $(y, 0)$.

   (a) Show: the affine transformation $p \to ap + b$ of E corresponds to the restriction of E^+ to the linear transformation
   $$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$
   and the affine vector field $p \to Xp + v$ on E corresponds to the restriction to E^+ of the linear vector field
   $$\begin{bmatrix} X & v \\ 0 & 0 \end{bmatrix}.$$

   (b) Show: the affine vector field $A : p \to Xp + v$ generates the one-parameter group of affine transformations
   $$\exp \tau A : p \to \exp(\tau X)p + \frac{\exp \tau X - 1}{X} v.$$
   [Start by explaining what this means.]

9. Let $X \in M$. Show:

   (a) There is exactly one trajectory for the vector field X through each point of E.

   (b) If $a \in \mathrm{GL}(E)$ commutes with X, then the transformation $E \to E$, $x \to ax$, permutes with the trajectories of X.

10. Let $X \in M$. Show:

    (a) For $p \in E$, $\exp(\tau X)p = p$ for all $\tau \in \mathbb{R}$ if and only if $X(p) = 0$. [In words: p is a stationary point of the flow, if and only if there is no current at p.]

    (b) If $\lim_{\tau \to \infty} \exp(\tau X)p_0 = p_\infty$ for some $p_0, p_\infty \in E$, then $Xp_\infty = 0$.

11. Two matrices P, Q are said to satisfy *Heisenberg's Commutation Relation* if

$$PQ - QP = k1$$

for some scalar k. Show that this is the case, if and only if

$$\exp \sigma P \exp \tau Q = e^{\sigma \tau k} \exp \tau Q \exp \sigma P$$

for all real σ, τ.

Appendix to §1.1: Notation and background

E denotes a n-dimensional real or complex vector space. Whenever necessary, we shall assume that E comes equipped with a positive definite inner product, written (x, y). We shall frequently have to express elements of E in terms of their components with respect to some basis and linear transformations of E in terms of their matrix coefficients. We could of course take E to be $\mathbb{R}^n$ or $\mathbb{C}^n$ from the outset, but this is of no help when one needs to choose a basis adapted to a particular situation rather than the standard basis. We therefore use the following expedient. Having fixed a basis (sometimes without mentioning this explicitly), we identify elements of E with (column) n-vectors and linear transformations of E with $n \times n$ matrices without change of notation. In this spirit, and in the interest of brevity, linear transformations of E are frequently referred to as *matrices*. The space of all linear transformations of E is denoted by $M = L(E)$ (*matrix space*). Elements of M are typically denoted X, Y, or Z when thought of as vector fields on E. Invertible linear transformations of E are usually denoted a, b, or c; they form the *general linear group* $\mathrm{GL}(E) = \{a \in L(E) | \det a \neq 0\}$ of all invertible linear transformations of E. $\mathrm{GL}(\mathbb{R}^n)$ and $\mathrm{GL}(\mathbb{C}^n)$ are also denoted $\mathrm{GL}(n, \mathbb{R})$ and $\mathrm{GL}(n, \mathbb{C})$, respectively.

A basis $\{e_k\}$ for E gives a basis $\{E_{ij}\}$ for the matrix space M consisting of the matrices E_{ij} with ij-entry 1 and 0 elsewhere. If e_k is orthonormal for the inner product (x, y) on E, then E_{ij} is orthonormal for the inner product (X, Y) on M given by

$$(X, Y) = \mathrm{tr}(Y^* X) = \sum_{ij} X_{ij} \bar{Y}_{ij}.$$

The asterisk denotes the adjoint with respect to the inner product (x, y) : $(Xx, y) = (x, X^* y)$. If X is represented as a matrix relative to an orthonormal basis, as above, then $X^* = \bar{X}^t$ (conjugate transpose).

The *matrix norm* in M is given by

$$\|X\|^2 = (X, X).$$

In terms of the orthonormal basis $\{E_{ij}\}$, $\|X\|^2$ is the usual sum of the squares of the absolute values entries of matrix X:

$$\|X\|^2 = \sum_{ij} |X_{ij}|^2.$$

It satisfies the inequalities

$$\|X+Y\| \le \|X\| + \|Y\|, \tag{A.1}$$
$$\|XY\| \le \|X\|\|Y\|. \tag{A.2}$$

The first of these is the familiar *triangle inequality*, which holds for any inner product space. The second one follows from the *Schwarz inequality* as follows: the ij-entry of XY, satisfies

$$\left|\sum_k X_{ik}Y_{kj}\right|^2 \le \left(\sum_l |X_{il}|^2\right)\left(\sum_l |Y_{lj}|^2\right)$$

the Schwarz Inequality. Summing over ij and taking the square root one gets (A.2).

A real vector space may always be thought of as the real subspace of a complex vector space of the same dimension, consisting of those vectors whose components with respect to a fixed basis are real. Similarly for real matrices. More formally, a real vector space E may be embedded in a complex vector space $E \oplus iE$ whose elements are formal sums $x+iy$, $x, y \in E$, added and multiplied by complex scalars in the obvious way. $E \oplus iE$ is called the *complexification* of E, denoted $E_{\mathbb{C}}$.

On the other hand, a complex vector space E may be considered as a real vector space (of twice the dimension) by forgetting about multiplication by i. The real and imaginary parts of the components of a vector in E relative to a complex basis $\{e_k\}$ are the components of the vector with respect to the real basis $\{e_k, ie_k\}$.

A linear transformation of a real vector space E extends uniquely to a linear transformation of its complexification $E_{\mathbb{C}}$. Both are represented by the same matrix with respect to a real basis for E considered also as a complex basis for $E_{\mathbb{C}}$. By the *eigenvalues* of a linear transformation of a real vector space E, we always mean the eigenvalues of the corresponding transformation of $E_{\mathbb{C}}$ (i.e. we always allow complex eigenvalues, as is customary).

As real vector space, M may be identified with $M_n(\mathbb{R}) = \mathbb{R}^{n\times n}$ or, if E is complex, with $M_n(\mathbb{C}) \approx \mathbb{R}^{2n\times 2n}$ (with the real and imaginary parts of the entries of complex matrices as real coordinates). Thus all notions from analysis on $\mathbb{R}^N$ apply to M without further comment. A special feature of analysis on the matrix space M are M-valued functions of a matrix variable $X \in M$ defined by matrix-power series:

$$\sum_{k=0}^{\infty} \alpha_k X^k. \tag{A.3}$$

A tail segment of such a series may be estimated by

$$\left\|\sum_{k=N}^{M} \alpha_k X^k\right\| \le \sum_{k=N}^{M} |\alpha_k|\,\|X^k\| \le \sum_{k=N}^{M} |\alpha_k|\,\|X\|^k, \tag{A.4}$$

obtained from the inequalities (A.1) and (A.2). From this, one sees that the matrix series (A.3) converges whenever $\sum_{k=0}^{\infty} |\alpha_k| \|X^k\|$ converges. One then says that the matrix series *converges in norm* or is *norm-convergent*. Such is in particular the case when the power series of norms $\sum_{k=0}^{\infty} |\alpha_k| \|X\|^k$ converges. Substituting τX for X into the series (A.3) one gets a power series in the scalar variable τ with coefficients depending on X:

$$\sum_{k=0}^{\infty} \alpha_k \tau^k X^k. \tag{A.5}$$

Generally, a power series with matrix coefficients, $\sum \tau^k A_k (A_k \in M)$, has a radius of (norm)-convergence $R \geq 0$ and may be treated according to the usual rules for scalar power series for $|\tau| < R$. For example, the series can be differentiated or integrated term-by-term with respect to τ within its radius of norm-convergence ($|\tau| < R$):

$$\frac{d}{d\tau}\left(\sum \tau^k A_k\right) = \sum k\tau^{k-1} A_k,$$
$$\int \left(\sum \tau^k A_k\right) d\tau = \sum \frac{\tau^{k+1}}{k+1} A_k + C.$$

For any matrix valued function $a(\tau)$ of a real variable τ (defined on some interval), the derivative $a'(\tau) = da/d\tau$ is defined by

$$a'(\tau) = \lim_{\epsilon \to 0} \frac{1}{\epsilon}(a(\tau + \epsilon) - a(\tau)), \tag{A.6}$$

whenever the limit exists. In addition to the usual rules for the derivative of vector valued functions one has the product rule

$$(ab)' = a'b + ab'. \tag{A.7}$$

This follows directly from the definition (A.6), since

$$(ab)(\tau + \epsilon) - (ab)(\tau) = (a(\tau + \epsilon) - a(\tau))b(\tau + \epsilon) + a(\tau)(b(\tau + \epsilon) - b(\tau)).$$

Note, incidentally, that the product rule (A.7) depends only on the fact that the matrix product ab is bilinear in a and b. The formula (A.7) therefore holds for any bilinear function $ab = f(a, b)$. The variables a and b and the value $f(a, b)$ may come from any (possibly different) vector spaces.

Where $\det a(\tau) \neq 0$, the inverse $a(\tau)^{-1}$ is differentiable and its derivative may be found by differentiating the relation $aa^{-1} = 1$ according to the rule (A.7), which gives:

$$\frac{da}{d\tau} a^{-1} + a \frac{da^{-1}}{d\tau} = 0,$$

hence

$$\frac{da^{-1}}{d\tau} = -a^{-1} \frac{da}{d\tau} a^{-1}.$$

Consult the appendix on Analytic Functions and the Inverse Function Theorem on page 250 for a review of these topics.

1.2 Ad, ad, and $d\exp$

We continue with exp, considered as a mapping $X \to \exp X$ of the matrix space M onto itself. First item:

Proposition 1. *The map* $\exp : M \to M$ *carries a neighbourhood of 0 one-to-one onto a neighbourhood of 1.*

More precisely, in a neighbourhood of 0, $\exp : M \to M$ has a local inverse[2] $\log : M \cdots\!\to M$, defined in a neighbourhood of 1 by the series

$$\log a = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}(a-1)^k. \tag{1}$$

This series converges in norm for $\|a-1\| < 1$, and

$$\log(\exp X) = X \quad \text{for } \|X\| < \log 2, \tag{2}$$

$$\exp(\log a) = a \quad \text{for } \|a-1\| < 1. \tag{3}$$

Proof. The series (1) converges in norm for $\|a-1\| < 1$ because

$$\sum_{k=1}^{\infty} \frac{1}{k}\|a-1\|^k,$$

converges for $\|a-1\| < 1$.

Working towards a proof of (2), we first try to calculate $\log(\exp X)$ naively by substituting the log series into the exp series:

$$\begin{aligned}\log(\exp X) &= \left(X + \frac{1}{2!}X^2 + \cdots\right) - \frac{1}{2}\left(X + \frac{1}{2!}X^2 + \cdots\right)^2 \\ &\quad + \frac{1}{3}\left(X + \frac{1}{2!}X^2 + \cdots\right)^3 + \cdots \\ &= X + \left(\frac{1}{2!}X^2 - \frac{1}{2}X^2\right) + \left(\frac{1}{3!}X^3 - \frac{1}{2}X^3 + \frac{1}{3}X^3\right) + \cdots \\ &= X + 0 + 0 + \cdots\end{aligned}$$

except that it is not immediately clear that the remaining dots are really all equal to 0. But one can argue as follows. First of all, since $\|\exp X - 1\| \le e^{\|X\|} - 1$, the double series for $\log(\exp X)$ converges in norm provided $e^{\|X\|} - 1 < 1$, i.e. $\|X\| < \log 2$. Assuming this, the terms of the double series for $\log(\exp X)$ may be rearranged at will. But then the coefficients of X^k must add up to 1 for $k = 1$ and to 0 otherwise, because this is the case when X is a scalar variable, and the operations on the coefficients are evidently the same whether X is thought of as a scalar or as a matrix. This proves (2); (3) is seen in the same way. QED

[2]The *broken arrow* $\cdots\!\to$ indicates a partially defined map, here and elsewhere.

The trick just used, though obvious, is worth recording:
Substitution Principle 2. Any equation involving power series in a variable X, which holds as an identity of absolutely convergent scalar series, also holds as an identity of norm-convergent matrix series. If the scalar series converge for $|X| < \rho$, then the matrix series converge for $\|X\| < \rho$.

Remark 2 (Substitution principle).
(a) A more detailed version of the Substitution Principle may be formulated as follows:

Let $F(z)$ and $G(z)$ be power series in a real or complex variable z with real or complex coefficients. Let $\sigma > 0$ be the radius of convergence of $F(z)$, $\rho > 0$ that of $G(z)$. Let $X \in M$ be a real or complex matrix. Then

(i) $(F+G)(X) = F(X) + G(X)$, if $\|X\| < \min(\sigma, \rho)$

(ii) $(FG)(X) = F(X)G(X)$, if $\|X\| < \min(\sigma, \rho)$

(iii) $(F \circ G)(X) = F(G(X))$, if $\|X\| < \rho$, $\|G(X)\| < \sigma$, and $G(0) = 0$.

The series $F+G$, FG, $F \circ G$ is defined by formal calculation the coefficients of this series. The condition $G(0) = 0$ in (iii) ensures that only finitely many coefficients of F and G contribute to a given coefficient of $F \circ G$.

The idea behind the Substitution Principle may apply even if the statement itself does not. For example, if X is a nilpotent matrix ($X^k = 0$ for some k), then $F(X)$ exists for any power series F, even though $\|X\|$ may lie outside its radius of convergence: consider $F(\tau X)$ as a power series in scalar variable τ. Some caution with the Substitution Principle is nevertheless advised, as one sees already from the equation $\log \exp z = z$ when one tries to substitute $z = 2\pi i$.

(b) The Substitution Principle extends in an obvious way to power series in several *commuting* matrices. All of the formulas of Proposition 1 of §1.1 could have been derived from the scalar case by the Substitution Principle in this form.

(c) The result of Proposition 1 is not the best possible. In fact, $\exp : M \to M, X \to a = \exp X$, maps the region of matrices X whose eigenvalues λ satisfy $|\mathrm{Im}\,\lambda| < \pi$ one-to-one onto the region of matrices whose eigenvalues α are *not* real and ≤ 0. These λ and α are in bijection under the complex exponential function $\alpha = \exp \lambda$. The assertion concerning matrices ultimately comes down to this. (See problem 3(c).) The notation log is also used for the inverse of exp on this larger domain, where series (1) need not converge.

There are two operations with matrices which are of importance in connection with exp. First, for any invertible $a \in M$ it is customary to denote by $\mathrm{Ad}(a)$ the conjugation operation by a as linear transformation of M:

$$\mathrm{Ad}(a)Y = aYa^{-1}.$$

Note that

$$\mathrm{Ad}(ab) = \mathrm{Ad}(a)\mathrm{Ad}(b), \quad \mathrm{Ad}(a^{-1}) = \mathrm{Ad}(a)^{-1},$$

so that Ad is a homomorphism from the group of invertible linear transformation of E to that of M:

$$\mathrm{Ad} : \mathrm{GL}(E) \to \mathrm{GL}(M).$$

This homomorphism is called the *adjoint representation* of $\mathrm{GL}(E)$. Second, in addition to big Ad, we introduce little ad by:

$$\mathrm{ad}(X)Y = XY - YX.$$

$\mathrm{ad}(X) : M \to M$ is a linear transformation of M defined for all $X \in M$ (invertible or not), and certainly not a group homomorphism. When thought of as an operation on matrices, $\mathrm{ad}(X)Y$ is also written as a *bracket*:

$$[X, Y] = XY - YX.$$

This bracket operation is evidently bilinear and skew-symmetric in X and Y; in addition it satisfies the *Jacobi Identity*

$$[[X, Y], Z] + [[Z, X], Y] + [[Y, Z], X] = 0.$$

(XYZ are permuted cyclically to form the terms of this sum.) It is equivalent to

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

which is called the *derivation property* of $\mathrm{ad}\, Z$. (The Jacobi Identity for matrices is verified by a simple calculation, which we omit. It derives its name from Jacobi's investigations in mechanics (1836).)

Big Ad and little ad are intertwined by exp in the following sense:

Proposition 4. *For any $X \in M$,*

$$\mathrm{Ad}(\exp X) = \exp(\mathrm{ad}\, X).$$

Explanation. There are two different exp's in this formula: on the left is exp of the linear transformation X of E, on the right, exp of the linear transformation $\mathrm{ad}\, X$ of M. Written out explicitly the formula says that for all $X, Y \in M$,

$$\exp(X)Y \exp(-X) = \sum_{k=0}^{\infty} \frac{1}{k!} (\mathrm{ad}\, X)^k Y.$$

Proof. Fix $X \in M$ and let $A(\tau) = \mathrm{Ad}(\exp \tau X)$ for $\tau \in \mathbb{R}$. Calculate its derivative:

$$\begin{aligned} A'(\tau)Y &= \frac{d}{d\tau}(\exp(\tau X)Y \exp(-\tau X)) \\ &= X \exp(\tau X)Y \exp(-\tau X) + \exp(\tau X)Y \exp(-\tau X)(-X) \\ &= (\mathrm{ad}\, X)\mathrm{Ad}(\exp \tau X)Y. \end{aligned}$$

Thus

$$A'(\tau) = U A(\tau)$$

with $U = \mathrm{ad}\, X$, and

$$A(0) = 1.$$

From Proposition 1 of §1.1 we know that the only solution of these equations is $A(\tau) = \exp(\tau U)$, which gives the desired result. QED

The next item is a differentiation formula for exp:

Theorem 5.

$$\frac{d}{d\tau}\exp X = \exp(X)\frac{1-\exp(-\operatorname{ad} X)}{\operatorname{ad} X}\frac{dX}{d\tau}.$$

Explanation. In this formula $X = X(\tau)$ is any matrix-valued differentiable function of a scalar variable τ. The fraction of linear transformations of M is defined by its (everywhere convergent) power series

$$\frac{1-\exp(-\operatorname{ad} X)}{\operatorname{ad} X} = \sum_{k=0}^{\infty}\frac{(-1)^k}{(k+1)!}(\operatorname{ad} X)^k.$$

The proposition may also be read as saying that the differential of $\exp : M \to M$ at any $X \in M$ is the linear transformation $d\exp_X : M \to M$ of M given by the formula

$$d\exp_X Y = \exp(X)\frac{1-\exp(-\operatorname{ad} X)}{\operatorname{ad} X}Y.$$

Historical Comment. The formula goes back to the beginnings of Lie theory. It was first proved by F. Schur (1891) (not to be confused with the better known I. Schur), and was taken up later from a different point of view by Poincaré (1899).

Proof. Let $X = X(\tau)$ be a differentiable curve in M and set

$$Y(\sigma,\tau) = (\exp -\sigma X(\tau))\frac{\partial}{\partial\tau}\exp\sigma X(\tau)$$

for $\sigma, \tau \in \mathbb{R}$. Differentiate with respect to σ:

$$\begin{aligned}
\frac{\partial Y}{\partial\sigma} &= (\exp -\sigma X)(-X)\frac{\partial}{\partial\tau}\exp(\sigma X) + \exp(-\sigma X)\frac{\partial}{\partial\tau}(X\exp\sigma X)\\
&= (\exp -\sigma X)(-X)\frac{\partial}{\partial\tau}\exp(\sigma X) + \exp(-\sigma X)\frac{dX}{d\tau}\exp(\sigma X)\\
&\quad + (\exp -\sigma X)X\frac{\partial}{\partial\tau}\exp(\sigma X)\\
&= (\exp -\sigma X)\frac{dX}{d\tau}\exp(\sigma X)\\
&= \operatorname{Ad}(\exp -\sigma X)\frac{dX}{d\tau}\\
&= \exp(\operatorname{ad} -\sigma X)\frac{dX}{d\tau}.
\end{aligned}$$

Now

$$\exp(-X)\frac{d}{d\tau}\exp X = Y(1,\tau) = \int_0^1 \frac{\partial}{\partial\sigma}Y(\sigma,\tau)\,d\sigma \quad [\text{since } Y(0,\tau) = 0]$$

and

$$\frac{\partial Y}{\partial \sigma} = (\exp -\sigma \operatorname{ad} X)\frac{dX}{d\tau} = \sum_{k=0}^{\infty} \frac{(-1)^k \sigma^k}{k!}(\operatorname{ad} X)^k \frac{dX}{d\tau}.$$

Integrate this series term-by-term from $\sigma = 0$ to $\sigma = 1$ to get

$$\exp(-X)\frac{d}{d\tau}\exp X = \sum_{k=0}^{\infty} \frac{(-1)^k}{(k+1)!}(\operatorname{ad} X)^k \frac{dX}{d\tau},$$

which is the desired formula. QED

The theorem, together with the Inverse Function Theorem (Appendix), gives information on the local behaviour of the exponential map: the Inverse Function Theorem says that exp has a local inverse around a point $X \in M$ at which its differential $d\exp_X$ is invertible, and the theorem says that this is the case precisely when $(1 - \exp(-\operatorname{ad} X))/\operatorname{ad} X$ is invertible, i.e. when zero is not an eigenvalue of this linear transformation of M. To find these eigenvalues we use a general result:

Lemma 6. *Let $f(z) = \sum_{k=0}^{\infty} \alpha_k z^k$ be a power series with real or complex coefficients. Suppose U is a linear transformation so that the series $f(U) = \sum_{k=0}^{\infty} \alpha_k U^k$ converges. If $\lambda_1, \lambda_2, \ldots, \lambda_N$ are the eigenvalues of U, listed with multiplicities, then $f(\lambda_1), f(\lambda_2), \ldots, f(\lambda_N)$ are the eigenvalues of $f(U)$, listed with multiplicities.*

Proof. Choose a basis so that U is triangular with diagonal entries $\lambda_1, \lambda_2, \ldots, \lambda_N$. (This may require passing to complex scalars, even if U starts out as a real linear transformation.) For each $k = 0, 1, \ldots, U^k$ is then also triangular with diagonal entries $\lambda_1^k, \lambda_2^k, \ldots, \lambda_N^k$. Thus, $f(U)$ itself is a triangular matrix with diagonal entries given by the power series $f(\lambda_1), f(\lambda_2), \ldots, f(\lambda_N)$; these power series $f(\lambda_j)$ converge, because $f(U)$ is assumed to converge. QED

From the lemma and the remarks preceding it one obtains now:

Proposition 7. *If none of the eigenvalues of $\operatorname{ad} X$ are of the form $\lambda = 2\pi i k$, $k = \pm 1, \pm 2, \ldots$, then $\exp : M \to M$ has a local inverse near X.*

Proof. By the lemma, the eigenvalues of $(1 - \exp -U)/U$ are of the form $(1 - e^{-\lambda})/\lambda$, λ an eigenvalue of U. The given values of λ are precisely the solutions of the equation $(1-e^{-\lambda})/\lambda = 0$; this gives the conclusion when one takes $U = \operatorname{ad} X$. QED

It remains to determine the eigenvalues of $\operatorname{ad} X$:

Lemma 8. *If X has n eigenvalues $\{\lambda_j | j = 1, 2, \ldots, n\}$, then $\operatorname{ad} X$ has n^2 eigenvalues $\{\lambda_j - \lambda_k | j, k = 1, 2, \ldots, n\}$.*

Proof. Let $\{e_j\}$ be a basis so that X is triangular, say

$$Xe_j = \lambda_j e_j + \cdots,$$

where the dots indicate a linear combination of e_k's with $k > j$. Let E_{jk} be the corresponding basis for M (E_{jk} has jk-entry 1 and all other entries 0). Order the basis E_{jk} of M so that $j - k < j' - k'$ implies E_{jk} precedes $E_{j'k'}$. One checks by matrix computation that

$$\mathrm{ad}(X)E_{jk} = (\lambda_j - \lambda_k)E_{jk} + \cdots,$$

where the dots indicate a linear combination of $E_{j'k'}$'s that come after E_{jk} in the chosen order. This means that $\mathrm{ad}(X)$ is triangular with diagonal entries $(\lambda_j - \lambda_k)$. QED

In view of Lemma 8, Proposition 7 can be rephrased as

Proposition 7′. If no two eigenvalues of $X \in M$ have a difference of the form $2\pi ik$, $k = 1, 2, \ldots$, then $\exp : M \to M$ has a local inverse near X.

Example 9 (exp **for real** 2×2 **matrices).** We start with the observation that for any matrix X

$$\det(\exp X) = e^{\mathrm{tr}\, X};$$

this is immediate from the formulas for det and tr in terms of eigenvalues. This formula implies first of all that any exponential of a real matrix must have a positive determinant. Furthermore, since $\exp(\alpha 1 + X) = e^{\alpha} \exp X$, it suffices to consider matrices with $\mathrm{tr}\, X = 0$, as far as the behaviour of the real matrix exponential is concerned.

We now specialize to the case of real 2×2 matrices. In view of the preceding remarks, we specialize further by *assuming throughout that* $\mathrm{tr}(X) = 0$. The characteristic polynomial of a 2×2 matrix X is

$$\det(\lambda 1 - X) = \lambda^2 - (\mathrm{tr}\, X)\lambda + (\det X)1.$$

According to Cayley–Hamilton,

$$X^2 - (\mathrm{tr}\, X)X + (\det X)1 = 0.$$

The assumption that $\mathrm{tr}\, X = 0$ implies $X^2 = -(\det X)1$. Use this fact to compute:

$$\begin{aligned}
\exp X &= \sum_{k=0}^{\infty} \frac{X^k}{k!} \\
&= \sum_{k=0}^{\infty} \frac{X^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{X^{2k+1}}{(2k+1)!} \\
&= \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} (\det X)^k 1 + \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} (\det X)^k X.
\end{aligned}$$

Recognizing these series one finds

$$\exp X = (\cos\sqrt{\det X})1 + \frac{\sin\sqrt{\det X}}{\sqrt{\det X}}X. \tag{4}$$

(The functions in (4) are independent of the choice of the sign of the root. The root may be imaginary; $\sin\theta$ and $\cos\theta$ are defined for complex arguments by:

$$\sin\theta = \tfrac{1}{2i}(e^{i\theta} - e^{-i\theta}), \quad \cos\theta = \tfrac{1}{2}(e^{i\theta} + e^{-i\theta}).$$

Looking at formula (4) more closely one sees:

For a 2×2 matrix a with $\det a = 1$, the equation $\exp X = a$ has a solution X if and only if $\frac{1}{2}\operatorname{tr} a > -1$ or $a = -1$. If so, the solutions are given as follows:

$$\text{(a) For } -1 < \tfrac{1}{2}\operatorname{tr} a < 1\text{:} \quad X = \frac{\xi}{\sin\xi}\left(a - \tfrac{1}{2}\operatorname{tr} a 1\right)$$

with $\xi > 0$ satisfying $\cos\xi = \frac{1}{2}\operatorname{tr} a$. There are countably many solutions.

$$\text{(b) For } \tfrac{1}{2}\operatorname{tr} a > 1\text{:} \quad X = \frac{\xi}{\sinh\xi}\left(a - \tfrac{1}{2}\operatorname{tr} a 1\right)$$

with $\xi > 0$ satisfying $\cosh\xi = \frac{1}{2}\operatorname{tr} a$. There is a unique solution.

$$\text{(c) For } \tfrac{1}{2}\operatorname{tr} a = 1,\ a \neq 1\text{:} \quad X = a - 1.$$

(d) $a = \pm 1$: $X =$ any matrix on one of the family of surfaces in the space of matrices 2×2 of trace zero is given by the equations

$$\det X = \begin{cases} (\pi 2k^2), & \text{if } a = +1 \\ (\pi(2k+1))^2, & \text{if } a = -1, k = 0, 1, 2, \ldots. \end{cases}$$

To get a better overview of the situation we introduce coordinates x, y, z in the three-dimensional space of a real 2×2 matrix X of trace zero, by setting

$$X = x\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + y\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + z\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Then $\det X = -\frac{1}{2}\operatorname{tr} X^2 = -x^2 - y^2 + z^2$. The region $\det X > 0$ inside the cone $\det X = 0$ consists of matrices of elliptic type. Under exp, they get mapped onto the region $\det a = 1$, $-1 < \frac{1}{2}\operatorname{tr} a < 1$ in a periodic way; the 'periods' are separated by the two-sheeted hyperboloids $\det X = (\pi k)^2$, $k = 1, 2, \ldots$, which themselves get collapsed to the points ± 1. The region $\det X < 0$ outside the cone consists of matrices of the hyperbolic type; they get mapped onto the region $\det a = 1$, $\frac{1}{2}\operatorname{tr} a > 1$ in a bijective way. The cone $\det X = 0$ consists of nilpotent matrices ($X^2 = 0$; parabolic type); they get mapped bijectively onto the unipotent matrices ($(a-1)^2 = 0$) (Figure 1).

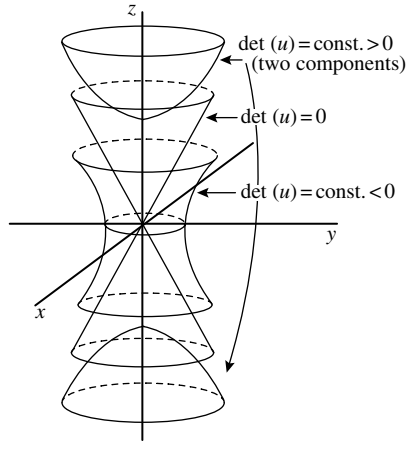

Fig. 1

These observations illustrate several results of this section. The equation

$$\exp(cXc^{-1}) = c(\exp X)c^{-1}$$

implies that exp maps the similarity class $\{cXc^{-1} | c \text{ an invertible } 2 \times 2 \text{ matrix}\}$ of X to the similarity class of $a = \exp X$. The similarity classes in $\{\operatorname{tr} X = 0\}$ are the surfaces $\det X = \text{const.}$, except for $X = 0$ on the cone $\det X = 0$. They are represented by the matrices

$$\begin{bmatrix} 0 & \theta \\ -\theta & 0 \end{bmatrix}, \quad \begin{bmatrix} \xi & 0 \\ 0 & -\xi \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{5}$$

with $\theta, \xi \neq 0$. The similarity classes in $\{\det a = 1\}$ are the surfaces $\frac{1}{2}\operatorname{tr} a = \text{const.}$, except for $a = \pm 1$ on $\frac{1}{2}\operatorname{tr} a = \pm 1$. They are represented by the matrices

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \quad \pm \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{6}$$

with $\theta \neq 2\pi k$, $k = 0, \pm 1, \pm 2, \ldots$ and $\alpha > 0$. The critical points of exp, those where its differential is singular, comprise the two-sheeted hyperboloids $\det X = (\pi k)^2$, $k = 1, 2, \ldots$ (represented by $\theta = \pi k$ in (5)); they get collapsed to the points ± 1. These are exactly the points where exp fails to be locally invertible, in agreement with the Inverse Function Theorem. The condition $\frac{1}{2}\operatorname{tr} a > -1$ or $a \neq -1$ excludes those similarity classes of 2×2 matrices a with $\det a = 1$ from the image of exp that are represented by

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}, \quad 0 < \alpha \neq 1, \quad -\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

In particular, $\exp : \{\operatorname{tr} X = 0\} \to \{\det a = 1\}$ is far from being surjective.

Problems for §1.2

1. A matrix $X \in M$ is called *nilpotent* if $X^k = 0$ for some k (equivalently: all eigenvalues of X are equal to 0); $a \in M$ is called *unipotent* if $(1-a)^k = 0$ for some k (equivalently: all eigenvalues of a are equal to 1). Show:

   $X \to \exp X$ maps the nilpotent matrices bijectively onto the unipotent matrices with inverse $a \to \log a$.

   [Proposition 1 does not apply directly, nor does the Substitution Principle as stated; a minor adjustment will do.]

2. A matrix a is called *semisimple* if it is diagonalizable over $\mathbb{C}$. Show:

   (a) $X \to \exp X$ maps semisimple matrices to semisimple matrices.

   (b) If a is an invertible semisimple matrix, then there is a semisimple matrix X so that $a = \exp X$ and no two distinct eigenvalues of X differ by a multiple of $2\pi i$.

   (c) Assume X and X' are both semisimple and no two distinct eigenvalues of X differ by a multiple of $2\pi i$. Show that $\exp X = \exp X'$ if and only if X and X' are *simultaneously* diagonalizable with diagonal entries differing by multiples of $2\pi i$.

   Any matrix X can be *uniquely* written as $X = Y + Z$ where Y is semisimple, Z is nilpotent, and Y and Z *commute*. Furthermore, Y and Z are linear combinations of powers of X. $X = Y + Z$ is called the *Jordan decomposition* of X. [See Hoffman–Kunze (1961) Theorem 8, page 217, for example.]

3. Show:

   (a) Any invertible matrix a can be *uniquely* written as $a = bc$ where b is semisimple, c is unipotent, and b and c *commute*. Furthermore, b and c are linear combination of powers of a.

   (b) If $X = Y + Z$ is the decomposition of X as in (a), then $\exp X = \exp Y \exp Z$ is the decomposition of $\exp X$ as in (b).

   (c) Assume that no two distinct eigenvalues of X differ by a multiple of $2\pi i$. (See problem 2(b)). Show that $\exp X = \exp X'$ if and only $Z = Z'$ and Y and Y' are simultaneously diagonalizable with diagonal entries differing by integral multiples of $2\pi i$. Deduce Remark 3(c).

4. Let λ be a non-zero complex number. Show that the matrix

$$\begin{bmatrix} \lambda & 1 & 0 \cdots & 0 \\ 0 & \lambda & 1 \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \cdots & \lambda \end{bmatrix}$$

is the exponential of a complex matrix. Deduce that every invertible complex matrix is an exponential. [Suggestion: For the second part, use the Jordan canonical form, which is the explicit version of the Jordan decomposition mentioned before problem 3.]

5. Show: not every matrix of determinant 1 is an exponential (real or complex) of a matrix of trace 0. Suggestion: Consider

$$\begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}.$$

6. Let $f(X) = \sum_k \alpha_k X^k$ be any matrix-power series. Use the Cayley–Hamilton Theorem to show that $f(X)$, can formally be rewritten as

$$f(X) = c_0(X) + c_1(X)X + \cdots + c_{n-1}(X)X^{n-1},$$

where the $c_j(X)$ are (multiple) power series in the matrix entries of X which are invariant under conjugation, i.e. $c_j(aXa^{-1}) = c_j(X)$. ['Formally' means 'do not worry about convergence when rearranging the series'].

7. Suppose $X \in M$ satisfies $\|X\| < 2\pi$. Show that for $v \in E$,

$$\exp(X)v = v \quad \text{if and only if } \; Xv = 0.$$

[Suggestion: the power series for $z/(\exp z - 1)$ converges for $|z| < 2\pi$].

8. (a) Prove the *Jacobi Identity*

$$[[X, Y], Z] + [[Z, X], Y] + [[Y, Z], X] = 0.$$

Deduce that
(b) $(\operatorname{ad} Z)[X, Y] = [(\operatorname{ad} Z)X, Y] + [X, (\operatorname{ad} Z)Y]$,
(c) $\operatorname{ad}([X, Y]) = [\operatorname{ad} X, \operatorname{ad} Y]$.
(The bracket on the right side of (c) is that of linear transformations of the matrix space M.)

9. Show that for all $X \in M$,

$$\exp X = \lim_{k\to\infty} \left(1 + \frac{1}{k}X\right)^k.$$

[The formula has a 'physical' interpretation: subdivide the time interval $0 \le \tau \le 1$ into a large number of subintervals k; the fluid particle travelling on the trajectory $p(\tau) = \exp(\tau X)p_0$, with velocity $Xp(\tau)$ at $p(\tau)$, will move from p_0 to approximately $p_0 + (1/k)Xp_0 = (1 + (1/k)X)p_0$ in the first time interval, on to $(1 + (1/kX))^2 p_0$ in the second, etc., until at $\tau = 1$ it reaches approximately $(1 + 1/kX)^k p_0$, which must therefore approximate $\exp(X)p_0$].

10. Prove the *Trotter Product Formula*: for all $X, Y \in M$,

$$\exp(X+Y) = \lim_{k\to\infty} \left(\exp\left(\frac{1}{k}X\right)\exp\left(\frac{1}{k}Y\right)\right)^k.$$

[Suggestion: start with $\exp(\tau X)\exp(\tau Y) = \exp(\tau(X+Y)+o(\tau))$.]

11. Let $\mathbb{R} \to M$, $\tau \to a(\tau)$, be a continuous map satisfying $a(\sigma+\tau) = a(\sigma)a(\tau)$ and $a(0) = 1$. Show that $a(\tau) = \exp \tau X$ for some $X \in M$. [This shows that the differentiability hypothesis on $a(\tau)$ in part (d) of Proposition 1 of §1.1 can be replaced by continuity. Suggestion for the proof: consider $X(\tau) = \log(a(\tau))$ for small τ. Show that $X(\rho\tau) = \rho X(\tau)$, first for $\rho = p/q$ rational, then for all $\rho \in \mathbb{R}$].

12. Fix $X \in M$. Let L be a subspace of M satisfying $[X, Y] \in L$ for all $Y \in L$. Show:

    (a) $\exp(\tau X)Y\exp(-\tau X) \in L$ for all $Y \in L$.

    (b) $\exp(-X)\exp(X+Y) \in 1 + L$ for all $Y \in L$.

    [Suggestion for (b): consider the tangent vector of the curve $a(\tau) = \exp(-X)\exp(X+\tau Y)$.]

13. Show that for any differentiable matrix valued function $a = a(\tau)$ of a real variable τ with $\det a(\tau) \neq 0$,

$$\frac{d}{d\tau}\det a = (\det a)\,\mathrm{tr}\left(a^{-1}\frac{da}{d\tau}\right).$$

[Suggestion: assume first $a(0) = 1$ and prove this formula at $\tau = 0$.]

1.3 The Campbell–Baker–Hausdorff series

In a neighbourhood of the identity matrix in M where exp has an inverse (e.g. on $\|a-1\| \leq 1$, where the log series converges) one may think of exp as providing a coordinate system: the matrix X (restricted to a neighbourhood of 0) serves as coordinate point of the matrix $a = \exp X$ (restricted to a neighbourhood of 1). We shall refer to these coordinates as *exponential coordinates*, without (for now) giving any further meaning to the term 'coordinates' in general. We need a formula for matrix multiplication in exponential coordinates; that is, we need a formula for the solution of the equation

$$\exp X \exp Y = \exp Z$$

for Z in terms of X and Y, at least for X, Y, Z in a neighbourhood of 0 in M, where this equation does have a unique solution, namely

$$Z = \log(\exp X \exp Y). \tag{1}$$

Expanding the right side of (1) we get

$$Z = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \left\{ \left(\sum_{i=0}^{\infty} \frac{X^i}{i!} \right) \left(\sum_{j=0}^{\infty} \frac{Y^j}{j!} \right) - 1 \right\}^k$$
$$= \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \left\{ \sum_{i,j \geq 0, i+j \geq 1} \frac{X^i Y^j}{i!j!} \right\}^k,$$

which leads to

$$Z = \sum \frac{(-1)^{k-1}}{k} \frac{X^{i_1} Y^{j_1} \cdots X^{i_k} Y^{j_k}}{i_1! j_1! \cdots i_k! j_k!} \tag{2}$$

where the sum is over all finite sequences $(i_1, j_1, \ldots, i_k, j_k)$ of integers ≥ 0 satisfying $i_r + j_r \geq 1$. The order of summation is unimportant as long as the series converges in norm when summed in *some* order, which is the case when $\sum (1/k)(e^{\|X\|} e^{\|Y\|} - 1)^k$ converges, i.e. when $\|X\| + \|Y\| < \log 2$.

The monstrosity (2) is extremely awkward to work with, but at least one can write out the first few terms:

$$Z = (X + Y + XY + \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2 + \cdots) - \tfrac{1}{2}(XY + YX + X^2 + Y^2 + \cdots) + \cdots$$
$$= X + Y + \tfrac{1}{2}(XY - YX) + \cdots .$$

Again we meet *the bracket* $[X, Y] = XY - YX$, *in terms of which*

$$Z = X + Y + \tfrac{1}{2}[X, Y] + \cdots . \tag{3}$$

The formula (2) gives the Taylor expansion of Z as function of X and Y; from (3) one sees that to the first order, Z is just the sum of X and Y, the second order term involves their bracket. It is truly a remarkable fact that the whole series (2) can be rewritten solely in terms of repeated brackets of X and Y. The proof, in hindsight quite simple, occupied several mathematicians: Campbell (1897), Poincaré (1899), Baker (1905), Hausdorff (1906), and Dynkin (1947). The first four addressed the question whether Z can be represented as a bracket series at all (which is the crux of the matter) without producing the explicit formula. (As Bourbaki (1972) puts it: "chacun considère que les démonstrations de ses prédécesseurs ne sont pas convaincantes'.) Dynkin finally gives the explicit formula, now generally (and somewhat paradoxically) known as 'Campbell–Baker–Hausdorff Series'. The proof given here follows Duistermaat–Kolk (1988); the essential ingredient is F. Schur's formula for the differential of exp (Theorem 5 of §1.2).

Theorem 1 (Dynkin's Formula). *For matrices $X, Y, Z \in M$ sufficiently close to 0, the equation*

$$\exp X \exp Y = \exp Z$$

has a unique solution for $Z = C(X, Y)$ as a convergent series in repeated brackets of X and Y, namely

$$C(X, Y) = \sum \frac{(-1)^{k-1}}{k} \frac{1}{(i_1 + j_1) + \cdots (i_k + j_k)} \frac{[X^{(i_1)} Y^{(j_1)} \cdots X^{(i_k)} Y^{(j_k)}]}{i_1! j_1! \cdots i_k! j_k!}. \tag{4}$$

Explanations and remarks. The sum is over all $2k$-tuples $(i_1, \dots, i_k, j_1, \dots, j_k)$ of integers ≥ 0 satisfying $i_r + j_r \geq 1$ with $k = 1, 2, \dots$. The brackets are defined as follows. For any finite sequence $X_1, \dots, X_k$ of matrices we set

$$[X_1, X_2, \dots, X_k] = [X_1, [X_2, \dots, [X_{k-1}, X_k], \dots]],$$

the brackets being inserted in the order shown. The expression

$$[X^{(i_1)} Y^{(j_1)} \dots X^{(i_k)} Y^{(j_k)}]$$

in (4) means the sequence starts with $i_1 X_1'$s, then $j_1 Y_1'$s etc. The convergence of (4) is not in question: if (4) is equal to (2), in the sense that the terms involving a given finite number of factors X, Y are equal, then (4) must converge for $\|X\| + \|Y\| < \log 2$, because (2) does, and must represent Z as long as $\|Z\| < 1$ (so that $\log(\exp Z)$ exists). Therefore the phrase 'sufficiently close to 0' may be interpreted more precisely as

$$\|X\| + \|Y\| < \log 2, \|Z\| < 1. \tag{5}$$

(Alternatively: compare (4) directly with the series expansion of $\sum_{k=0}^{\infty}(1/k)$ $(e^{\alpha} e^{\beta} - 1)$ using $\|[X, Y]\| < 2\|X\| \, \|Y\|$. In this way, one need not know (2) = (4) to prove the convergence of (4).)

Actually, the exact expression of Z in terms of X and Y is of little importance and will not be used later. What is of importance is that Z can be written as a bracket series in X and Y in some way. The exact formula is given mainly to dispel the air of mystery from the qualitative statement.

Of course, at this point it is not at all clear what is to be gained by writing the complicated series (2) in the even more complicated form (4). Certainly, as far as actual computations are concerned, the formula (4) is hardly practical; its significance is theoretical: the whole edifice of Lie theory ultimately rests on this formula (at least on its qualitative form).

Proof. Fix X, Y and let $Z = Z(\tau)$ be the solution of

$$\exp(Z) = \exp(\tau X) \exp(\tau Y). \tag{6}$$

Differentiate using Theorem 5 of §1.2:

$$\exp(Z) \frac{1 - \exp(-\operatorname{ad} Z)}{\operatorname{ad} Z} \frac{dZ}{d\tau} = X \exp(Z) + \exp(Z) Y$$

or

$$\frac{dZ}{d\tau} = \frac{-\operatorname{ad} Z}{1 - \exp(\operatorname{ad} Z)} X - \frac{\operatorname{ad} Z}{1 - \exp(\operatorname{ad} Z)} \exp(\operatorname{ad} Z) Y. \tag{7}$$

Equation (6) gives

$$\exp(\operatorname{ad} Z) = \exp(\operatorname{ad} \tau X) \exp(\operatorname{ad} \tau Y), \tag{8}$$

(Proposition 4 of §1.2). Now use the power series expansions

$$A = \log(1 + (\exp A - 1)) = \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} (\exp A - 1)^{k+1}. \tag{9}$$

Apply (9) with $A = \operatorname{ad} Z$ to the fractions in (7) and apply (8) to the term $\exp(\operatorname{ad} Z)Y$ in (7) and compute as in the derivation of (2):

$$\begin{aligned}
\frac{dZ}{d\tau} &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} \{(\exp(\operatorname{ad}\tau X)\exp(\operatorname{ad}\tau Y) - 1)^k X \\
&\quad + (\exp(\operatorname{ad}\tau X)\exp(\operatorname{ad}\tau Y) - 1)^k \exp(\operatorname{ad}\tau X) Y\} \\
&= \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} \left\{ \sum \tau^{i_1+j_1+\cdots+i_k+j_k} \frac{[X^{(i_1)}Y^{(j_1)} \dots X^{(i_k)}Y^{(j_k)}X]}{i_1 j_1! \cdots i_k! j_k!} \right. \\
&\quad \left. + \tau^{i_1+j_1+\cdots+i_k+j_k+i_{k+1}} \frac{[X^{(i_1)}Y^{(j_1)} \dots X^{(i_k)}Y^{(j_k)}X^{(i_{k+1})}Y]}{i_1! j_1! \cdots i_k! j_k! i_k + 1!} \right\}.
\end{aligned} \tag{10}$$

Integrate expression term-by-term (using $Z(0) = 0$):

$$Z(1) = \int_0^1 \frac{dZ}{d\tau} d\tau.$$

This gives the desired relation (4) after shifting the index of summation. One also needs to observe that the general term of (4) is zero unless j_k equals 0 or 1, which corresponds to the two terms in (10). QED

We close this section with a few formulas, which follow from Campbell–Baker–Hausdorff, but are actually better proved directly.

Proposition 2.

(a) $\exp(X)\exp(Y) = \exp(X + Y + \frac{1}{2}[X, Y] + \cdots)$

(b) $\exp(X)\exp(Y)\exp(-X) = \exp(Y + [X, Y] + \cdots)$

(c) $\exp(X)\exp(Y)\exp(-X)\exp(-Y) = \exp([X, Y] + \cdots)$

where the dots indicate terms involving products of three or more factors X, Y.

Proof.
(a) is a restatement of equation (3), although a simpler proof may be given if this is all one wants: one only needs to compare terms of order ≤ 2 in $\exp(X)\exp(Y) = \exp Z$, Z written as a power series in X, Y with unknown coefficients.

(b) This is seen either by writing

$$\exp(X)\exp(Y)\exp(-X) = \exp\left(\exp(\operatorname{ad} X)Y\right)$$

and writing out the first few terms of the inner exp, or by using (a) twice:

$$\begin{aligned}\exp(X)\exp(Y)\exp(-X) &= \exp(X+Y+\tfrac{1}{2}[X,Y]+\cdots)\exp(-X)\ \text{[once]}\\ &= \exp(Y+[X,Y]+\cdots)\text{[twice]}\end{aligned}$$

(c) Same method. QED

Problems for §1.3

1. Prove part (c) of Proposition 2.

2. Use Dynkin's formula (4) to show that

$$C(X,Y) = X+Y+\tfrac{1}{2}[X,Y]+\tfrac{1}{12}[X,[X,Y]]+\tfrac{1}{12}[Y,[Y,X]]+\cdots .$$

Check that this agrees with what one obtains by writing out the terms up to order three of the series (4).

3. Prove that the series C(X,Y) can also be written in the following form:

$$C(X,Y) = \sum \frac{(-1)^k}{k+1}\frac{1}{i_1+\cdots+i_k+1}\frac{[X^{(i_1)}Y^{(j_1)}\dots X^{(i_k)}Y^{(j_k)}X]}{i_1!j_1!\cdots i_k!j_k!}.$$

[Suggestion: Start with $Z = Z(\tau)$ defined by $\exp(Z) = \exp(\tau X)\exp(Y)$ instead of (6); imitate the proof. Comment: this formula might seem slightly simpler than (4), but is equally unmanageable and less symmetric. If one reverses the roles of X and Y in this procedure one obtains a formula reflecting the relation $C(-Y,-X) = -C(X,Y)$, which is evident form the definition of $C(X,Y)$].

4. Write $\exp(Z) = \exp(\tau X)\exp(\tau Y)$ as in (6). Let

$$Z = \sum_k \tau^k C_k,$$

be the expansion of Z in powers of τ. Derive the recursion formula

$$(k+1)C_{k+1} = -[C_k, X] + \sum \gamma_j [C_{k_1}\cdots[C_{k_j}, X+Y]\cdots],$$

where the γ_j are defined as the coefficients of the series

$$\frac{x}{1-e^{-x}} = \sum_j \gamma_j x^j.$$

(Compare with the *Bernoulli numbers* β_j defined by

$$\frac{x}{e^x-1} = \sum_j \beta_j \frac{x^j}{j!},$$

i.e. $\gamma_j = (-1)^j\beta_j/j!$).

[Suggestion: Show first that

$$\frac{dZ}{d\tau} = -\operatorname{ad}(Z)X + \frac{\operatorname{ad} Z}{1-\exp(-\operatorname{ad} Z)}(X+Y).$$

Then substitute power series.]

A *linear Lie algebra* is a space $\mathfrak{n} \subset M$ of linear transformations that is closed under the bracket operation:

$$X, Y \in \mathfrak{n} \quad \text{implies} \quad [X, Y] \in \mathfrak{n}.$$

5. Let $\mathfrak{n}$ be a linear Lie algebra consisting of *nilpotent* matrices. Let $N = \{\exp \mathfrak{n} = \exp X | X \in \mathfrak{n}\}$. Show that N is a *group* under matrix multiplication, i.e.

$$a \in N \quad \text{implies} \quad a^{-1} \in N,$$
$$a, b \in N \quad \text{implies} \quad ab \in N.$$

[Suggestion: for $a = \exp X$ and $b = \exp Y$, consider $Z(\tau)$ defined by $\exp(\tau X)\exp(\tau Y) = \exp Z(\tau)$ as a power series in τ with matrix coefficients. All nilpotent $n \times n$ matrices A satisfy $A^n = 0$.]

6. Let $\mathfrak{n}_1$ and $\mathfrak{n}_2$ be two linear Lie algebras consisting of nilpotent matrices as in problem 5, N_1 and N_2 be the corresponding groups. Let $\varphi : \mathfrak{n}_1 \to \mathfrak{n}_2$ be a linear map. Show that the rule $f(\exp X) = \exp \varphi(X)$ defines a *group homomorphism* $f : N_1 \to N_2$ (i.e. a well-defined map satisfying $f(ab) = f(a)f(b)$ for all $a, b \in N_1$) if and only if $\varphi([X, Y]) = [\varphi X, \varphi Y]$ for all $X, Y \in \mathfrak{n}_1$.

Problems 7 and 8 are meant to illustrate problems 5 and 6. Assume known the results of those problems.

7. (a) Describe all subspaces $\mathfrak{n}$ consisting of nilpotent upper triangular matrices real 3×3 matrices

$$\begin{bmatrix} 0 & \alpha & \gamma \\ 0 & 0 & \beta \\ 0 & 0 & 0 \end{bmatrix}$$

which satisfy $[\mathfrak{n}, \mathfrak{n}] \subset \mathfrak{n}$. Describe the corresponding groups N.

(b) Give an example of a subspace $\mathfrak{n}$ of M with $[\mathfrak{n}, \mathfrak{n}] \subset \mathfrak{n}$ for which $N = \exp \mathfrak{n}$ is *not* a group. [Suggestion: Consider Example 9 of §1.2.]

8. Let $\mathfrak{n}$ be the space of all nilpotent upper triangular real $n \times n$ matrices

$$\begin{bmatrix} 0 & * & * \cdots & * \\ 0 & 0 & * \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \cdots & 0 \end{bmatrix}. \tag{1}$$

Then $N = \exp \mathfrak{n}$ consists of all unipotent upper triangular real $n \times n$ matrices

$$\begin{bmatrix} 1 & * & * \cdots & * \\ 0 & 1 & * \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 \cdots & 1 \end{bmatrix}.$$

Let $\varphi : \mathfrak{n} \to \mathbb{R}$ be a linear functional. Show that the rule

$$f(\exp X) = e^{\varphi(X)}$$

defines a group homomorphism $f : N \to \mathbb{R}^\times$ of N onto the group $\mathbb{R}^\times$ of non-zero reals under multiplication if and only if $\varphi(\mathfrak{n}') = 0$, where $\mathfrak{n}'$ is the subspace of $\mathfrak{n}$ of matrices with entries zero directly above the main diagonal.

9. Compare the series (2) and (4):

$$Z = \sum \frac{(-1)^{k-1}}{k} \frac{X^{i_1} Y^{j_1} \cdots X^{i_k} Y^{j_k}}{i_1! j_1! \cdot i_k! j_k!}, \tag{2}$$

$$C(X,Y) = \sum \frac{(-1)^{k-1}}{k} \frac{1}{(i_1 + j_1) + \cdots (i_k + j_k)} \frac{[X^{(i_1)} Y^{(j_1)} \ldots X^{(i_k)} Y^{(j_k)}]}{i_1! j_1! \cdots i_k! j_k!}. \tag{3}$$

This problem 'explains' the evident formal relation between the two through an outline of Dynkin's original proof.

Let A denote the collection of all formal *polynomials* (finite formal series) in the non-commuting formal variables X, Y. A is a real vector space with a basis consisting of the (infinitely many) distinct *monomials* in the list $X^{i_1} Y^{j_1} \cdots X^{i_k} Y^{j_k}, i_r, j_r = 0, 1, 2, \ldots$. Elements of A are multiplied in the obvious way, and we define a bracket in A by the formula

$$[a, b] = ab - ba.$$

This bracket is real-bilinear, skew-symmetric, and satisfies the Jacobi Identity

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0.$$

Let L be the subspace of A spanned by all repeated brackets of X's and Y's, including the elements X and Y themselves. It is clear that $[a, b]$ is in L whenever a and b are. Define a map $\gamma : A \to L$ by

$$\gamma(1) = 0, \qquad \gamma(X) = X, \qquad \gamma(Y) = Y,$$

and generally

$$\gamma(X^{i_1} Y^{j_1} \cdots X^{i_k} Y^{j_k}) = [X^{(i_1)} Y^{(j_1)} \cdots X^{(i_k)} Y^{(j_k)}],$$

the right side being interpreted as explained in connection with formula (4). For each $a \in A$ define a linear map $\delta(a) : A \to A$ by

$$\delta(1)c = c, \qquad \delta(X)c = [X, c], \qquad \delta(Y)c = [Y, c],$$

and generally

$$\delta(X^{i_1}Y^{j_1} \cdots X^{i_k}Y^{j_k})c = \delta(X)^{i_1}\delta(Y)^{j_1} \cdots \delta(X)^{i_k}\delta(Y)^{j_k}c.$$

These operations obey the rules

$$\delta(ab) = \delta(a)\delta(b),$$
$$\gamma(ab) = \delta(a)\gamma(b),$$

which follow directly from the definitions. Prove:

(a) If $a \in L$, then $\delta(a)b = [a, b]$.

(b) If $a, b \in L$, then $\gamma([a, b]) = [\gamma(a), b] + [a, \gamma(b)]$.

(c) If $a \in L$ is homogeneous of degree m, then $\gamma(a) = ma$.

Explanation. $a \in A$ is *homogeneous of degree* m if it is a linear combination of terms

$$X^{i_1}Y^{j_1} \cdots X^{i_k}Y^{j_k} \tag{4}$$

with $i_1 + j_1 + \cdots + i_k + j_k = m$. [Suggestion: It suffices to consider homogeneous elements. Use induction on the degree.]

Written as $a = (1/m)\gamma(a)$, the rule (c) says: a homogeneous polynomial of degree m which can be written as a bracket series in *some* way, remains unchanged if we replace each monomial therein by the corresponding bracket monomial and divide by m. If this recipe is applied to the homogeneous terms of the series (2), assuming known that this series does lie in L (as was indeed the case historically), there results the series (4).