Summer Research Project Report
The University of Auckland, Department of Mathematics

An Investigation into Geometry of Möbius Transformations with a foundation in Complex Analysis, Geometry, Algebra and Lie Theory

under Dr. Pedram Hekmati

Anish Sachdeva
Delhi Technological University (DTU)
February 2020

Contents

1 Dramatis Personae

Augustin Louis Cauchy
(1898–1962)

Bernhard Reiman
(1591–1661)

Carl Friedrich Gauss
(1928–2014)

Felix Klien
(1862–1943)

Karl Weierstrass
(1910–1999)

Vladmir V. Kisil
(1882–1935)

2 Complex Numbers

2.1 Complex Number System

There is no real number x that satisfies the polynomial equation $x^2 + 1 = 0$. To permit solutions of this and similar equations, the set of Complex Numbers is introduced. We consider a complex number as having the form $a + ib$ where a and b are real numbers and i, which is called the imaginary unit, has the property that $i^2 = -1$. If $z = a + ib$ then a is called the real part of z and b is called the imaginary part of z denoted by $Re\{z\}$ and $Im\{z\}$ respectively. The symbol z which can stand for any Complex number denotes a complex variable.

Two complex numbers $a + ib$ and $c + id$ are called equal if and only if $a = c$ and $b = d$. We can consider the set of all real numbers $\mathbb{R}$ as a subset of complex numbers where $b = 0$.

The complex conjugate or briefly conjugate of a Complex Number $a + ib$ is denoted by $\bar{z} = a - ib$. Can sometimes also be indicated by z^*

2.2 Fundamental Operations and Absolute Value

(1) Addition

$$(a + bi) + (c + di) = (a + b) + (c + d)i$$

(2) Subtraction

$$(a + bi) - (c + di) = (a - b) + (c - d)i$$

(3) Multiplication

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

(4) Division

If $c \neq 0$ and $d \neq 0$, then

$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di}\frac{c - di}{c - di} = \frac{ac + bd}{c^2 + dr} + \frac{bc - ad}{c^2 + d^2}i$$

(5) Absolute Valueor Modulus

The absolute value or modulus of a complex number $a+bi$ is defined as $|a+bi| = \sqrt{a^2 + b^2}$. If $z_1, z_2, \ldots z_m$ are all complex numbers the following properties hold true:

1. $|z_1 z_2| = |z_1||z_2|$ or $|z_1 z_2 \ldots z_m| = |z_1||z_2| \ldots |z_m|$
2. $|\frac{z_1}{z_2}| = \frac{|z_1|}{|z_2|}$ if $|z_2| \neq 0$
3. $|z_1 +_2 | \leq |z_1| + |z_2|$ or $|z_1 + z_2 + \cdots + z_m| \leq |z_1| + |z_2| + \cdots + |z_m|$
4. $|z_1 \pm z_2| \geq |z_1| - |z_2|$

2.3 De Moivre's Theorem

Let $z_1 = x_1 + iy_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = x_2 + iy_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ then we can show that

$$z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)) \tag{1}$$

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)) \tag{2}$$

A generalization of (1) leads us to

$$z_1 z_2 \ldots z_n = r_1 r_2 \ldots r_n(\cos(\theta_1 + \theta_2 + \cdots + \theta_n) + i\sin(\theta_1 + \theta_2 + \cdots + \theta_n)) \tag{3}$$

and if $z_1 = z_2 = \cdots = z_n = z$, equation (3) becomes

$$z^n = r^n(\cos n\theta + i\sin n\theta) \tag{4}$$

And (4) is often referred to as De-moivre's Theorem

2.4 Roots of Complex Number

A number w is called the nth root of a complex number z if $w^n = z$, and we write $w = z^{1/n}$. From De-Moivre's theorem we can show that if n is a positive integer

$$z^{1/n} = r^{1/n}(\cos\theta + i\sin\theta)^{1/n}$$

$$z^{1/n}\{\cos(\frac{\theta + 2k\pi}{n}) + i\sin(\frac{\theta + 2k\pi}{n})\} \tag{5}$$

$$\text{where } k = 0, 1, 2 \ldots n-1$$

from which it follows that there are n different values for $z^{1/n}$, i.e. n different nth roots of z provided $z \neq 0$.

2.5 Euler's Formula

By assuming that the infinite series expansion of e^x is given by

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$

By plugging in $x = i\theta$ we arrive at the following result

$$e^{i\theta} = \cos\theta + i\sin\theta \tag{6}$$

which is called Euler's Formula, however it is simply more convenient to take (6) as the definition of $e^{i\theta}$. In general we define

$$e^z = e^{x+iy} = e^x e^{iy} = e^x(\cos y + i\sin y) \tag{7}$$

In the special case where $y = 0$ this reduces to e^x and from the De-Moivre's Theorem in (4) we can also see that reduces to $(e^{i\theta})^n = e^{in\theta}$

2.6 The nth Roots of Unity

The solutions of the equation $z^n = 1$ where n is a positive integer are called the nth roots of unity and are given by

$$z = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{2ki\pi/n} \tag{8}$$

$$\text{where } k = 0, 1, 2 \ldots n-1$$

If we let $\omega = \cos 2\pi/n + i\sin 2\pi/n = e^{2\pi i/n}$, then the n roots are $1, \omega, \omega^2, \ldots, \omega^{n-1}$. Geometrically they represent the n vertices of a regular polygon of n sides inscribed in a circle of radius one with center at the origin. This circle has the equation $|z| = 1$ and is often called the unit circle.

2.7 Point Sets

Any collection of Points in the complex plane is called a (two-dimensional) point set, and each point is called a member or element of this set. the following fundamental definitions in resoect to the complex-plane are:

1. **Neighbourhoods:** A *delta*, or δ neighbourhood of a point z_0 is the set of all points z such that $|z - z_0| < \delta$ where δ is any given positive number. A deleted δ neighbourhood of z_0 is a neighbourhood of z_0 in which the point z_0 is omitted i.e. $0 < |z - z_0| < \delta$.

2. **Limit Point:** A point z_0 is called a limit point, cluster point or a point of accumulation of a point set S if every deleted δ neighbourhood z_0 contains point S. Since δ can be any positive number it follows that S must have infinitely many points. Note that z_0 may or may not belong to the set S.

3. **Closed Sets:** A set S is said to be closed if every limit point of S belongs to S, i.e. if set S contains all limit points. For example, the set of all points z such that $|z| \leq 1$ is a closed set.

4. **Bounded Sets:** A set S is called a Bounded Set if we can find a constant M such that $|z| < M$ for every point z in S. An unbounded set is one which is not bounded. A set which is both bounded and closed is called compact.

5. **Interior, Exterior and Boundary Points:** A point z_0 is called an interior point of a set S if we can find a δ neighbourhood of z_0 all of whose points belong to S. If every δ neighbourhood of z_0 contains points belonging to S and also points not belonging to S, then z_0 is called a boundary point.If a point is not an interior or boundary point of set S, it is an exterior point of set S.

6. **Open Sets:** An open set is a set which consists only of interior points. For example the set of points z such that $|z| < 1$ is an open set.

7. **Connected Sets:** An Open set S is said to be connected if any 2 points of the set can be joined by a path consisting of straight line segments (i.e. a polygonal path) all points of which are in S.

8. **Open Regions or Domains:** An open connected set is called an open region or domain.

9. **Closure of a Set:** If to a set S we add all the limit points of S, the new set is called the closure of S and is a closed set.

10. **Closed Regions:** The closure of an open region or domain is called a closed region.

11. **Regions:** If to an open region or domain we add some, all or none of its limit points, we obtain a set called a region. If all the limit points are added, the region is closed; if none are added, the region is open. In this book whenever we use the word region without qualifying it, we shall mean open region or domain.

12. **Union and Intersection of Sets:** A set consisting of all points belonging to set S_1 or set S_2 or to both sets S_1 and S_2 is called the union of S_1 and S_2 and is denoted by $S1 \cup S2$. A set consisting of all points belonging to both sets S_1 and S_2 is called the intersection of S_1 and S_2 and is denoted by $S_1 \cap S_2$.

13. **Complement of a Set:** A set consisting of all points which do not belong to S is called the complement of S and is denoted by $\tilde{S}$ or S^c.

14. **Null Sets and Subsets:** Null Sets and Subsets. It is convenient to consider a set consisting of no points at all. This set is called the null set and is denoted by ϕ. If two sets S_1 and S_2 have no points in common (in which case they are called disjoint or mutually exclusive sets), we can indicate this by writing $S_1 \cap S_2 = \phi$. Any set formed by choosing some, all or none of the points of a set S is called a subset of S. If we exclude the case where all points of S are chosen, the set is called a proper subset of S.

15. **Countability of a Set:** Suppose a set is finite or its elements can be placed into a one to one correspondence with the natural numbers 1, 2, 3, ... Then the set is called countable or denumerable; otherwise it is non-countable or non-denumerable.

2.8 Weirstrass-Bolzanno Theorem

Every bounded infinite set has at least one limit point.

2.9 Heine–Borel Theorem

Let S be a compact set each point of which is contained in one or more of the open sets $A_1, A_2, \ldots$ [which are then said to cover S]. Then there exists a finite number of the sets $A_1, A_2, \ldots$ which will cover S.

3 Functions, Limits and Continuity

3.1 Variables and Functions

A symbol, such as z, which can stand for any one of a set of complex numbers is called a complex variable. Suppose, to each value that a complex variable z can assume, there corresponds one or more values of a complex variable w. We then say that w is a function of z and write $w = f(z)$ or $w = G(z)$ etc. The variable z is sometimes called an independent variable, while w is called a dependent variable. The value of a function at $z = a$ is often written $f(a)$. Thus, if $f(z) = z^2$, then $f(2i) = (2i)^2 = -4$.

3.2 Single and multiple-valued Functions

If only one value of w corresponds to each value of z, we say that w is a single-valued function of z or that $f(z)$ is single-valued. If more than one value of w corresponds to each value of z, we say that w is a multiple valued or many-valued function of z. A multiple-valued function can be considered as a collection of single-valued functions, each member of which is called a branch of the function. It is customary to consider one particular member as a principal branch of the multiple-valued function and the value of the function corresponding to this branch as the principal value.

3.3 Inverse Functions

If $w = f(z)$, then we can also consider z as a function, possibly multiple-valued, of w, written $z = g(w) = f^{-1}(w)$. The function f^{-1} is often called the inverse function corresponding to f. Thus, $w = f(z)$ and $w = f^{-1}(z)$ are inverse functions of each other.

3.4 Transformation

If $w = u + iv$ (where u and v are real) is a single-valued function of $z = x + iy$ (where x and y are real), we can write $u + iv = f(x + iy)$. By equating real and imaginary parts, this is seen to be equivalent to

$$u = u(x, y) \text{ and } v = v(x, y)$$

3.5 Limits

Let $f(z)$ be defined and single-valued in a neighborhood of $z = z_0$ with the possible exception of $z = z_0$ itself (i.e. in a deleted d neighborhood of z_0). We say that the number l is the limit of $f(z)$ as z approaches z_0 and write $\lim_{z\to z_0} f(z) = l$ if for any positive number ϵ (however small), we can find some positive number δ (usually depending on ϵ) such that $|f(z) - l| < \epsilon$ whenever $0 < |z - z_0| < \delta$. In such a case, we also say that $f(z)$ approaches l as z approaches z_0 and write $f(z) \to l$ as $z \to z_0$. The limit must be independent of the manner in which z approaches z_0. Geometrically, if z_0 is a point in the complex plane, then $\lim_{z\to z_0} f(z) = l$ if the difference in absolute value between $f(z)$ and l can be made as small as we wish by choosing points z sufficiently close to z_0 (excluding $z = z_0$ itself). //

When the limit of a function exists, it is unique. If $f(z)$ is multiple-valued, the limit as $z \to z_0$ may depend on the particular branch.

3.6 Theorem on Limits

Suppose $\lim_{z\to z_0} f(z) = A$ and $\lim_{z\to z_0} g(z) = B$. Then

1. $\lim_{z\to z_0}(f(z) + g(z)) = \lim_{z\to z_0} f(z) + \lim_{z\to z_0} g(z) = A + B$
2. $\lim_{z\to z_0}(f(z) - g(z)) = \lim_{z\to z_0} f(z) - \lim_{z\to z_0} g(z) = A - B$
3. $\lim_{z\to z_0} f(z)g(z) = (\lim_{z\to z_0} f(z))(\lim_{z\to z_0} g(z)) = AB$
4. $\lim_{z\to z_0} \frac{f(z)}{g(z)} = \frac{\lim_{z\to z_0} f(z)}{\lim_{z\to z_0} g(z)} = \frac{A}{B}$ if $B \neq 0$

3.7 Continuity

Let $f(z)$ be defined and single-valued in a neighborhood of $z = z_0$ as well as at $z = z_0$ (i.e. in a δ neighborhood of z_0). The function $f(z)$ is said to be continuous at $z \to z_0$ if $\lim_{z\to z_0} f(z) = f(z_0)$. Note that this implies three conditions that must be met in order that $f(z)$ be continuous at $z \to z_0$:

1. $\lim_{z\to z_0} f(z) = l$ must exist
2. $f(z_0)$ must exist
3. $l = f(z_0)$

Points in the z plane where $f(z)$ fails to be continuous are called discontinuities of $f(z)$ and $f(z)$ is said to be discontinuous at these points. If $\lim_{z\to z_0} f(z)$ exists but is not equal to $f(z_0)$, we call z_0 a removable discontinuity since by redefining $f(z_0)$ to be the same as $\lim_{z\to z_0} f(z)$ the function becomes continuous.

An alternatively to the above definition of continuity , we can define $f(z)$ as continuous at $z = z_0$ if for any $\epsilon > 0$, we can find $\delta > 0$ such that $|f(z) - f(z_0)| < \epsilon$ whenever $|z - z_0| < \delta$.

Note that this is simply the definition of limit with $l = f(z_0)$ and removal of the restriction that zz_0.

To examine the continuity of $f(z)$ at $z = \infty$, we let $z = 1/w$ and examine the continuity of $f(1/w)$ at $w = 0$

3.8 Continuity In a Region

A function $f(z)$ is said to be continuous in a region if it is continuous at all points of the region.

3.9 Uniform Continuity

Let $f(z)$ be continuous in a region. Then by definition at each point z_0 of the region and for any $\epsilon > 0$ we can find $\delta > 0$ (which will in general depend on both ϵ and the particular point z_0) such that $|f(z) - f(z_0)| < \epsilon$ whenever $|z - z_0| < \delta$. If we can find δ depending on ϵ but not on particular point z_0, we say that $f(z)$ is uniformly continuous in the region.

Alternatively $f(z)$ is uniformly continuous in the region for any $\epsilon > 0$ we can find $\delta > 0$ such that $|f(z_1) - f(z_2)| < \epsilon$ for $|z_1 - z_2| < \delta$ where z_1 and z_2 are two points in the region.

4 Complex Differentiation and the Cauchy-Riemann Equations

4.1 Derivatives

If $f(z)$ is single-valued in some region R of the z plane, the derivative of $f(z)$ is defined as

$$f^{'}(z) = \lim_{\Delta z \to 0} \frac{f(z + \Delta z) - f(z)}{\Delta z} \tag{9}$$

provided that the limit exists independent of the manner in which $\Delta z \neq 0$. In such a case, we say that $f(z)$ is differentiable at z. In the definition (9), we sometimes use h instead of Δz. Although differentiability implies continuity, the reverse is not true.

4.2 Analytic Functions

If the derivative $f^{'}(z)$ exists at all points z of a region R, then $f(z)$ is said to be analytic in R and is referred to as an analytic function in R or a function analytic in R. The terms regular and holomorphic are sometimes used as synonyms for analytic. A function $f(z)$ is said to be analytic at a point z_0 if there exists a neighborhood $|z - z_0| < \delta$ at all points of which $f^{'}(z)$ exists.

4.3 Cauchy-Riemann Equations

A necessary condition that $w = f(z) = u(x, y) + iv(x, y)$ be analytic in a region R is that, in R, u and v satisfy the Cauchy–Riemann equations.

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x} \tag{10}$$

If the partial derivatives in (10) are continuous in R, then the Cauchy–Riemann equations are sufficient conditions that $f(z)$ be analytic in R. The functions $u(x, y)$ and $v(x, y)$ are sometimes called conjugate functions. Given u having continuous first partials on a simply connected region R, we can find v (within an arbitrary additive constant) so that $u + iv = f(z)$ is analytic.

4.4 Harmonic Functions

If the second partial derivatives of u and v with respect to x and y exist and are continuous in a region R, then we find from (10) that

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0, \qquad \frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} = 0 \tag{11}$$

It follows from both these equations that the real and imaginary parts of the analytic function must satisfy Lapalace's equation denoted by:

$$\frac{\partial^2 \Psi}{\partial x^2} + \frac{\partial^2 \Psi}{\partial y^2} = 0 \quad \text{or} \quad \nabla^2 \Psi = 0 \quad \text{where} \quad \nabla^2 = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \tag{12}$$

The operator ∇^2 is often called the Laplacian. Functions such as $u(x, y)$ and $v(x, y)$ which satisfy the Laplace's equation in a region R are called *Harmonic Functions* and are said to be *Harmonic* in R.

4.5 L'Hospital's Rule

Let $f(z)$ and $g(z)$ be analytic in a region containing the point z_0 and suppose that $f(z_0) = g(z_0) = 0$ but $g^{'}(z_0) = 0$. Then, L'Hospital's rule states that:

$$\lim_{z \to z_0} \frac{f(z)}{g(z)} = \lim_{z \to z_0} \frac{f^{'}(z)}{g^{'}(z)} = \frac{f^{'}(z_0)}{g^{'}(z_0)} \tag{13}$$

In the case of $f^{'}(z_0) = g^{'}(z_0) = 0$, the rule may be extended.

4.6 Singular Points

A point at which $f(z)$ fails to be analytic is called a *singular point* or *singularity* of $f(z)$. Various types of singularities exist.

1. **Isolated Singularities:** The point $z = z_0$ is called an *isolated singularity* or *isolated singular point* of $f(z)$ if we can find $\delta > 0$ such that the circle $|z - z_0| < \delta$ encloses no singular point other than z_0 (i.e., there exists a deleted δ neighborhood of z_0 containing no singularity). If no such δ can be found, we call z_0 a non-isolated singularity.

   If z_0 is not a singular point and we can find $\delta > 0$ such that $|z - z_0| = \delta$ encloses no singular point, then we call z_0 an *ordinary point* of $f(z)$.

2. **Poles:** If z_0 is an isolated singularity and we can find a positive integer n such that $\lim_{z \to z_0}(z - z_0)^n f(z) = A \neq 0$, then $z = z_0$ is called a pole of order n. If $n = 1$, z_0 is called a *simple pole*.

   Examples:

   (a) $f(z) = 1/(z - 2)^3$ has a pole of order 3 at $z = 2$.

   (b) $f(z) = (3z - 2)/(z - 1)^2(z + 1)(z - 4)$ has a pole of order 2 at $z = 1$ and simple poles at $z = -1$ and $z = 4$

   If $g(z) = (z - z_0)^n f(z)$, where $f(z_0) \neq 0$ and n is a positive integer, then $z = z_0$ is called the *zero of order* n of $g(z)$. If $n = 1$, z_0 is called a *simple zero*. In such a case z_0 is pole of order n on the function $1/g(z)$.

5 Complex Integration and Cauchy's Theorem

5.1 Real Line Integrals

Let P(x, y) and $Q(x, y)$ be real functions of x and y continuous at all points of curve C. Then the real line integral of $Pdx + Qdy$ along curve C can be defined and is denoted by:

$$\int_C P(x, y)dx + Q(x, y)dy \quad \text{or} \quad \int_C Pdx + Qdy \tag{14}$$

The second notation being used for brevity. If C is smooth and has parametric equations $x = \phi(t)$ and $y = \psi(t)$ where $t_1 \leq t \leq t_2$, it can be shown that the value of (14) is given by

$$\int_{t_1}^{t_2} [P(\phi(t), \psi(t))\phi^{'}(t)dt + Q(\phi(t), \psi(t))\psi^{'}(t)dt] \tag{15}$$

Suitable modifications can be made if C is piecewise smooth.

5.2 Connection Between Real and Complex Line Integrals

Suppose $f(z) = u(x, y) + iv(x, y) = u + iv$. Then the complex line integral can be expressed in terms of real line integrals as follows

$$\int_C f(z)dz = \int_C (u + iv)(dx + i\ dy) = \int_C u\ dx - v\ dy + i \int_C v\ dx + u\ dy \tag{16}$$

5.3 Properties of Integrals

Suppose $f(z)$ and $g(z)$ are integrable along C. Then the following hold:

1. $\int_C f(z) + g(z)dz = \int_C f(z)dz + \int_C g(z)dz$
2. $\int_C Af(z)dz = A \int_C f(z)dz$ where A is an constant
3. $\int_a^b f(z)dz = -\int_b^a f(z)dz$
4. $\int_a^b f(z)dz = \int_a^m f(z)dz + \int_m^b f(z)dz$
5. $|\int_C f(z)dz| \leq M$ where $|f(z)| \leq M$ i.e. M is the upper bound of $f(z)$ on C, and L is length of C.

5.4 Simply and Multiple Connected Regions

A region R is called simply-connected if any simple closed curve, which lies in R, can be shrunk to a point without leaving R. A region R, which is not simply-connected, is called multiplyconnected. For example, suppose R is the region defined by $|z| < 2$ shown shaded below. If Γ is any simple closed curve lying in R [i.e., whose points are in R], we see that it can be shrunk to a point that lies in R, and thus does not leave R, so that R is simply-connected. On the other hand, if R is the region defined by $1 < |z| < 2$, shown shaded below, then there is a simple closed curve Γ lying in R that cannot possibly be shrunk to a point without leaving R, so that R is multiply-connected.

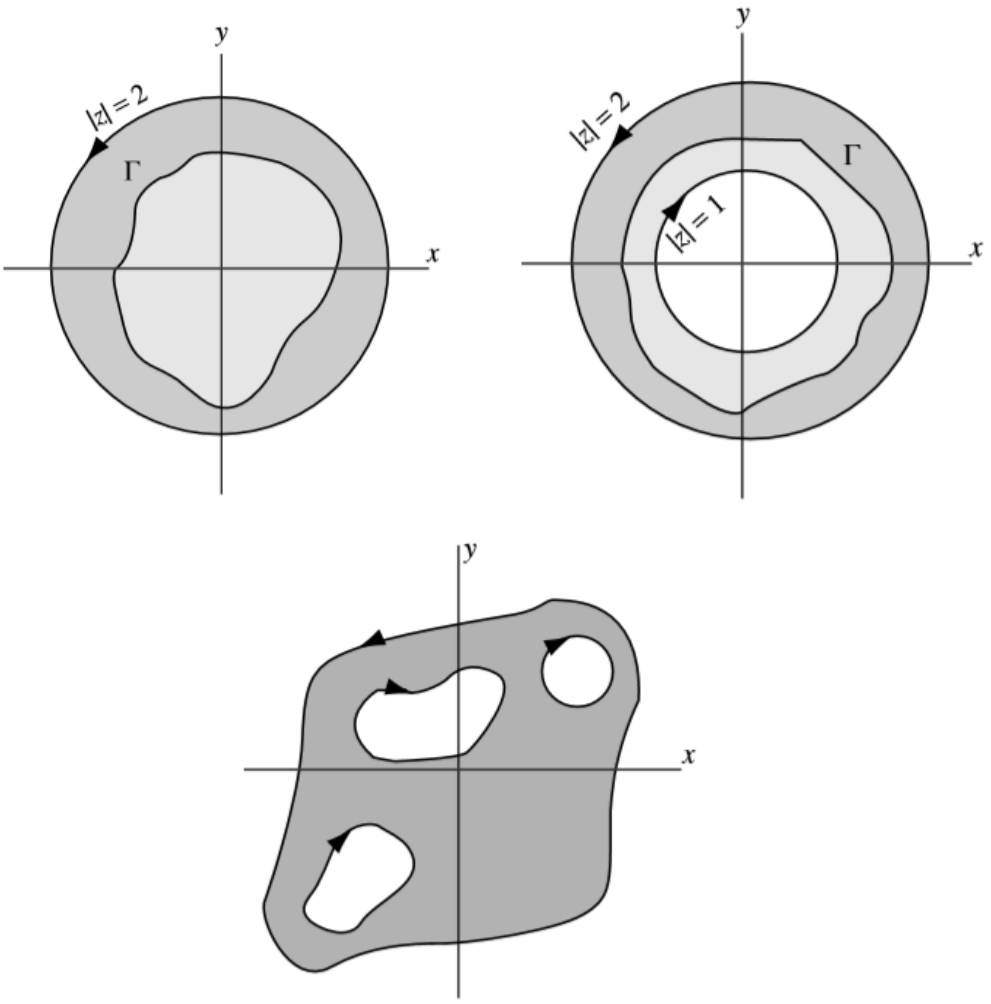


Figure 1: Multiple Connected and Simple Regions

Intuitively, a simply-connected region is one that does not have any "holes" in it, while a multiplyconnected region is one that does.

5.5 Jordan Curve Theorem

Any continuous, closed curve that does not intersect itself and may or may not have a finite length, is called a Jordan curve. An important theorem that, although very difficult to prove, seems intuitively obvious is the following. Jordan Curve Theorem. A Jordan curve divides the plane into two regions having the curve as a common boundary. That region, which is bounded [i.e., is such that all points of it satisfy $|z| < M$ where M is some positive constant], is called the interior or inside of the curve, while the other region is called the exterior or outside of the curve. Using the Jordan curve theorem, it can be shown that the region inside a simple closed curve is a simply-connected region whose boundary is the simple closed curve.

5.6 Convention Regarding Traversal of Closed Paths

The boundary C of a region is said to be traversed in the positive sense or direction if an observer travelling in this direction [and perpendicular to the plane] has the region to the left. This convention leads to the directions indicated by the arrows in Fig. 1 We use the special symbol

$$\oint_C f(z)dz$$

to denote integration of $f(z)$ around the boundary C in the positive sense. In the case of a circle, the positive direction is the counterclockwise direction. The integral around C is often called a *contour integral*.

5.7 Green's Theorem in a Plane

Let $P(x, y)$ and $Q(x, y)$ be continuous and have continuous partial derivatives in a region R and on its boundary C. Green's theorem states that

$$\oint_C P\,dx + Q\,dy = \iint_R (\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y})dxdy \tag{17}$$

The theorem is valid for both simply- and multiply-connected regions.

5.8 Complex Form of Green's Theorem

Let $F(z, \bar{z})$ be continuous and have continuous partial derivatives in a region R and on its boundary C, where $z = x + iy$, $\bar{z} = x - iy$ are complex conjugate coordinates. Then Green's theorem can be written in the complex form as

$$\int_C F(z, \bar{z})dz = 2i \iint_R \frac{\partial F}{\partial \bar{z}} dA \tag{18}$$

where dA represents the element of area $dx\,dy$.

5.9 Cauchy's Theorem and the Cauchy-Goursast Theorem

Let $f(z)$ be analytic in a region R and on its boundary C. Then

$$\oint_C f(z)dz = 0 \tag{19}$$

This fundamental theorem, often called Cauchy's integral theorem or simply Cauchy's theorem, is valid for both simply- and multiply-connected regions. It was first proved by use of Green's theorem with the added restriction that $f'(z)$ be continuous in R. However, Goursat gave a proof which removed this restriction. For this reason, the theorem is sometimes called the Cauchy–Goursat theorem when one desires to emphasize the removal of this restriction.

This is a very fundamental and important theorem and will be used later as the basis of mnay important results and calculations.

5.10 Morera's Theorem

Let $f(z)$ be continuous in a simply-connected region R and suppose that

$$\oint_C f(z)dz = 0$$

around every simple closed curve C in R. Then $f(z)$ is analytic in R. This theorem, due to Morera, is often called the converse of Cauchy's theorem. It can be extended to multiply-connected regions.

5.11 Some Consequences of Cauchy's Theorem

Let $f(z)$ be analytic in a simply-connected region R. Then the following theorems hold.

1. **Theorem 5.1** Suppose a and z are any two points in R. Then

$$\int_a^z f(z)dz$$

is independent of the path in R joining a and z.

2. **Theorem 5.2** Suppose a and z are any two points in R and

$$G(z) = \int_a^z f(z)dz$$

Then $G(z)$ is analytic in R and $G^{'}(z) = f(z)$.

Occasionally, confusion may arise because the variable of integration z in (Theorem 5.2) is the same as the upper limit of integration. Since a definite integral depends only on the curve and limits of integration, any symbol can be used for the variable of integration and, for this reason, we call it a dummy variable or dummy symbol. Thus (Theorem 5.2) can be equivalently written

$$G(z) = \int_a^z f(\epsilon)d\epsilon$$

3. **Theorem 5.3** Suppose a and b are any two points in R and $F^{'}(z) = f(z)$. Then

$$\int_a^b f(z) = F(b) - F(a)$$

4. **Theorem 5.4** Let $f(z)$ be analytic in a region bounded by two simple closed curves C and C_1 [where C_1 lies inside C] and on these curves. Then

$$\oint_C f(z)dz = \oint_{C_1} f(z)dz$$

where C and C_1 are both traversed in the positive sense relative to their interiors. The result shows that if we wish to integrate $f(z)$ along curve C, we can equivalently replace C by any curve C_1 so long as $f(z)$ is analytic in the region between C and C_1 as shown in figure 5.2.

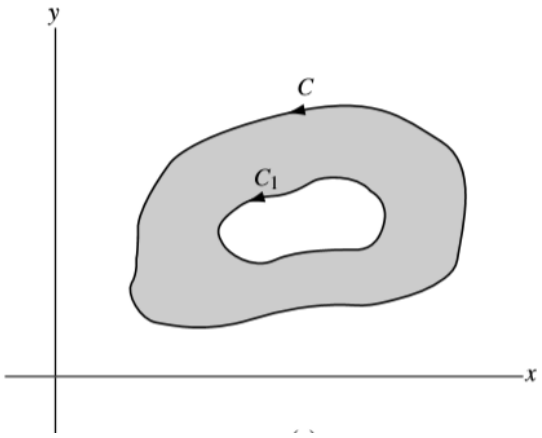


Figure 5.2: A closed curve inside another another closed curve

5. **Theorem 5.5** Let $f(z)$ be analytic in a region bounded by the non-overlapping simple closed curves C, C_1, C_2, C_3, $\ldots C_n$ where C_1, $C_2 \ldots C_n$ are inside C [as in Fig. 5.3] and on these curves. Then

$$\int_C f(z)dz = \int_{C_1} f(z)dz + \int_{C_2} f(z)dz + \int_{C_3} f(z)dz + \cdots + \int_{C_n} f(z)dz$$

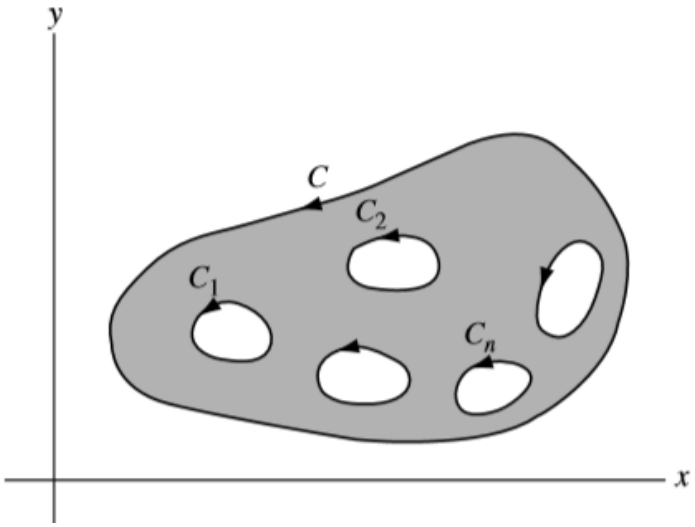


Figure 5.3: Multiple non-overlapping simple closed curves in a region

This is a generalization of the Theorem 5.4

6 Cauchy's Integral Formulas and Related Theorems

6.1 Cauchy's Integral Formula

Let $f(z)$ be analytic inside and on a simple closed curve C and let a be any point inside C [Fig. 6.1]. Then

$$f(a) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{z-a} dz \tag{20}$$

where C is traversed in the positive (counterclockwise) sense. Also, the nth derivative of $f(z)$ at $z = a$ is given by

$$f^{(n)}(a) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{(z-a)^{n+1}} dz \quad mn = 1, 2, 3 \ldots \tag{21}$$

The result (21) can be considered a special case of (20) with $n = 0$ if we define $0! = 1$.

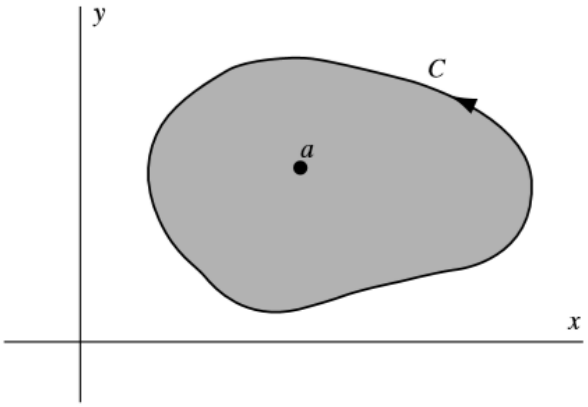


Figure 6.1: Simply Connected Region inside a closed contour with no holes

The results (20) and (21) are called Cauchy's integral formulas and are quite remarkable because they show that if a function $f(z)$ is known on the simple closed curve C, then the values of the function and all its derivatives can be found at all points inside C. Thus, if a function of a complex variable has a first derivative, i.e., is analytic, in a simply-connected region R, all its higher derivatives exist in R. This is not necessarily true for functions of real variables.

6.2 Some Important Theorems

The following is a list of some important theorems that are consequences of Cauchy's integral formulas.

1. **Morera's Theorem** (converse of Cauchy's theorem) If $f(z)$ is continuous in a simply-connected region R and if $\oint_C f(z)dz = 0$ around every simple closed curve C in R, then $f(z)$ is analytic in R.

2. **Cauchy's Inequality** Suppose $f(z)$ is analytic inside and on a circle C of radius r and center at $z = a$. Then

$$|f^{(n)}(a)| \leq \frac{M\dot{n}!}{r^n} \quad n = 0, 1, 2 \ldots \tag{22}$$

   where M is a constant such that $|f(z)| < M$ on C i.e. M is an upper bound of $|f(z)|$ on C.

3. **Liouville's theorem** Suppose that for all z in the entire complex plane

   (a) $f(z)$ is analytic

   (b) $f(z)$ is bounded

   i.e. $|f(z)| < M$ for some constant M. Then $f(z)$ must be a constant.

4. **Fundamental Theorem of Algebra** Every polynomial equation $P(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = 0$ with degree $n \geq 1$ and $a_n \neq 0$ has at least one root. From this it follows that $P(z) = 0$ has exactly n roots, due attention being paid to multiplicities of roots.

5. **Gauss' mean value theorem** Suppose $f(z)$ is analytic inside and on a circle C with center at a and radius r. Then $f(a)$ is the mean of the values of $f(z)$ on C, i.e.,

$$f(a) = \frac{1}{2\pi} \int_0^{2\pi} f(a + re^{i\theta}) d\theta \tag{23}$$

6. **Maximum modulus theorem** Suppose $f(z)$ is analytic inside and on a simple closed curve C and is not identically equal to a constant. Then the maximum value of $|f(z)|$ occurs on C.

7. **Minimum modulus theorem** Suppose $f(z)$ is analytic inside and on a simple closed curve C and $f(z) = 0$ inside C. Then $|f(z)|$ assumes its minimum value on C.

8. **The Argument Theorem** Let $f(z)$ be analytic inside and on a simple closed curve C except for a finite number of poles inside C. Then

$$\frac{1}{2\pi i} \oint_C \frac{f'(z)}{f(z)} dz = N - P \tag{24}$$

   where N and P are, respectively, the number of zeros and poles of $f(z)$ inside C.

9. **Rouche 's theorem** Suppose $f(z)$ and $g(z)$ are analytic inside and on a simple closed curve C and suppose $|g(z)| < |f(z)|$ on C. Then $f(z) + g(z)$ and $f(z)$ have the same number of zeros inside C.

6.3 Meromorphic Functions

A function that is analytic everywhere in the finite plane except at a finite number of poles is called a *meromorphic function.*

Example: $z/(z-1)(z+3)^2$ which is analytic everywhere in the finite plane except at the poles $z = 1$ (simple pole) and $z = -3$ (pole of order 2), is a meromorphic function.

7 Residue Theorem Evaluation of Integral and Series

7.1 Residues

Let $f(z)$ be single-valued and analytic inside and on a circle C except at the point $z = a$ chosen as the center of C. Then, we know, $f(z)$ has a Laurent series about $z = a$ given by

$$\begin{aligned} f(z) &= \Sigma_{n=-\infty}^{\infty} a_n (z-a)^n \\ &= a_0 + a_1(z-a) + a_2(z-a)^2 + \cdots + \frac{a_{-1}}{z-a} + \frac{a_{-2}}{(z-a)^2} + \dots \end{aligned}$$

where

$$a_n = \frac{1}{2\pi i} \oint_C \frac{f(z)}{(z-a)^{n+1}} dz \quad n = 0, \pm 1, \pm 2 \dots$$

In the special case $n = -1$ we have

$$\oint_C f(z) dz = 2\pi i a_{-1}$$

We call a_{-1} the residue of $f(z)$ at $z = 1$.

7.2 Calculation of Residues

To obtain the residue of a function $f(z)$ at $z = a$, it may appear that the Laurent expansion of $f(z)$ about $z = a$ must be obtained. However, in the case where $z = a$ is a pole of order k, there is a simple formula for a_{-1} given by

$$a_{-1} = \lim_{z \to a} \frac{1}{(k-1)!} \frac{d^{k-1}}{dz^{k-1}} ((z-a)^k f(z)) \tag{25}$$

If $k = 1$ (simple pole), the results are especially simple and are given by

$$a_{-1} = \lim_{z \to a} (z-a) f(z) \tag{26}$$

7.3 The Residue Theorem

Let $f(z)$ be single-valued and analytic inside and on a simple closed curve C except at the singularities $a, b, c, \ldots$ inside C, which have residues given by $a_{-1}, b_{-1}, c_{-1}, \ldots$ [see Fig. 7.1]. Then, the residue theorem states that

$$\oint_C f(z)dz = 2\pi i(a_{-1} + b_{-1} + c_{-1} + \ldots) \tag{27}$$

i.e., the integral of $f(z)$ around C is $2\pi i$ times the sum of the residues of $f(z)$ at the singularities enclosed by C. Note that (27) is a generalization of the case with simple pole and single residue. Cauchy's theorem and integral formulas are special cases of this theorem.

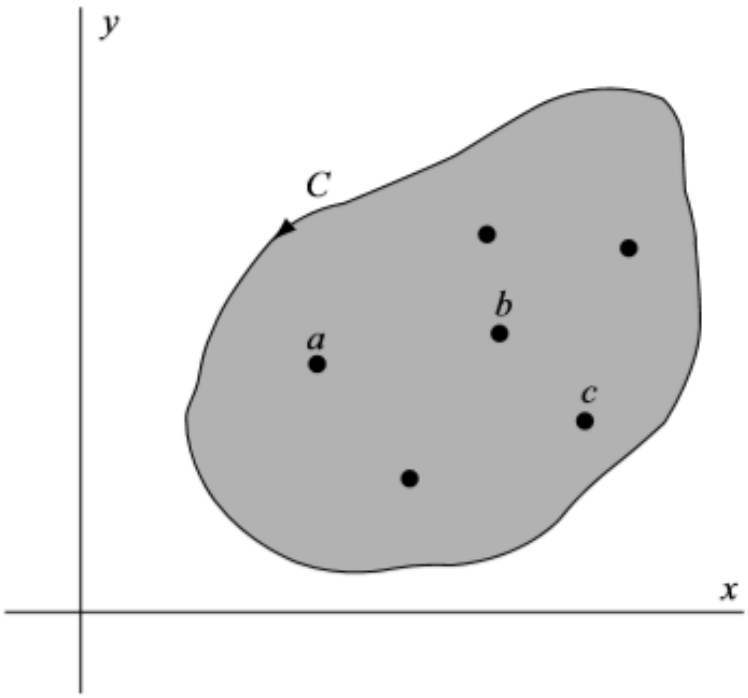


Figure 7.1: A region with multiple singular points

8 Conformal Mappings

8.1 Transformations or Mappings

The set of equations

$$\begin{aligned} u &= u(x, y) \\ v &= v(x, y) \end{aligned} \tag{28}$$

defines, in general, a transformation or mapping, which establishes a correspondence between points in the uv and xy planes. The equations (28) are called transformation equations. If to each point of the uv plane, there corresponds one and only one point of the xy plane, and conversely, we speak of a one-to-one transformation or mapping. In such a case, a set of points in the xy plane (such as a curve or region) is mapped into a set of points in the uv plane (curve or region) and conversely. The corresponding sets of points in the two planes are often called images of each other.

8.2 Complex Mapping Function

A case of special interest occurs when u and v are real and imaginary parts of an analytic function of a complex variable $z = x + iy$, i.e., $w = u + iv = f(z) = f(x + iy)$. In such a case, the Jacobian of the transformation is given by

$$\frac{\partial(u, v)}{\partial(x, y)} = |f^{'}(z)|^2 \tag{29}$$

It follows that the transformation is one-to-one in regions where $f^{'}(z) = 0$. Points where $f^{'}(z) = 0$ are called critical points.

8.3 Fixed or Invariant Points of a Transformation

Suppose that we superimpose the w plane on the z plane so that the coordinate axes coincide and there is essentially only one plane. Then we can think of the transformation $w = f(z)$ as taking certain points of the plane into other points. Points for which $z = f(z)$ are called the fixed or invariant points of the transformation.

Example: The fixed or invariant points of the transformation $w = z^2$ are solutions of $z^2 = z$, i.e., $z = 0, 1$.

8.4 Some General Transformations

In the following, α , β are given complex constants while a, θ_0 are real constants.

1. **Translation:** $w = z + \beta$
   By this transformation, figures in the z plane are displaced or translated in the direction of vector β.

2. **Rotation:** $w = e^{i\theta_0} z$
   By this transformation, figures in the z plane are rotated through an angle θ_0. If $_0 > 0$, the rotation is counterclockwise while, if $\theta_0 < 0$, the rotation is clockwise.

3. **Stretching:** $w = az$
   By this transformation, figures in the z plane are stretched (or contracted) in the direction z if $a < 1$ (or $0 < a < 1$). We consider contraction as a special case of stretching.

4. **Inversion:** $w = 1/z$

8.5 The Linear Transformation

The transformation

$$w = \alpha z + \beta \tag{30}$$

where α and β are given complex constants, is called *Linear Transformation*. Let $\alpha = e^{i\theta_0}$, we see that a general linear transformation is the combination of the transformations of translation, rotation, and stretching.

8.6 The Bilinear or Fractional Transformation

The transformation

$$w = \frac{\alpha z + \beta}{\gamma z + \delta} \quad \text{where} \quad \alpha\delta - \beta\gamma \neq 0 \tag{31}$$

is called a bilinear or fractional transformation. This transformation can be considered as a combination of the transformations of translation, rotation, stretching, and inversion.

The transformation (31) has the property that circles in the z plane are mapped into circles in the w plane, where by circles we include circles of infinite radius that are straight lines. These transformatiosn we will see later are also referred to as the Möbius Transformations and will study more properties and features after a refresher on Group Theory, Lie Groups and Algebra.

The transformation maps any three distinct points of the z plane into three distinct points of the w plane, one of which may be at infinity. If z_1, z_2, z_3, z_4 are distinct, then the quantity

$$\frac{(z_4 - z_2)(z_2 - z_3)}{(z_2 - z_1)(z_4 - z_3)} \tag{32}$$

is called the cross ratio of z_1, z_2, z_3, z_4. This ratio is invariant under the bilinear transformation, and this property can be used in obtaining specific bilinear transformations mapping three points into three other points.

9 Introduction to Group Theory and basic definitions in Groups and Algebra

9.1 Notation

We use the standard (Bourbaki) notations: $\mathbb{N} = \{0, 1, 2 \dots\}$
$\mathbb{Z}$ is the ring of integers
$\mathbb{Q}$ is the field of rational numbers
$\mathbb{R}$ is the field of real numbers;
C is the field of complex numbers;

$\mathbb{F}_q$ is a finite field with q elements where q is a power of a prime number. In particular, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p a prime number. For integers m and n, $m|n$ means that m divides n, i.e., $n \in m\mathbb{Z}$.

Throughout the notes, p is a prime number, i.e., $p = \{2, 3, 5, 7, 11, \dots, 1000000007, \dots\}$ Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. The empty set is denoted by ϕ. The cardinality of a set S is denoted by $|S|$ (so $|S|$ is the number of elements in S when S is finite).

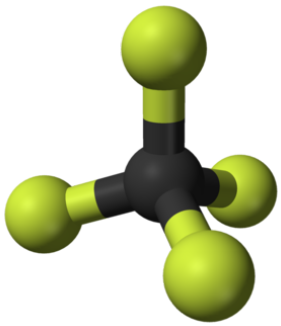
Let I and A be sets; a family of elements of A indexed by I , denoted by $(a_i)_{i \in I}$, is a function $i \hookrightarrow a_i : I \longrightarrow A$

Rings are required to have an identity element e, and homomorphisms of rings are required to take 1 to 1. An element a of a ring is a unit if it has an inverse (element b such that $ab = 1 = ba$). The identity element of a ring is required to act as 1 on a module over the ring.

9.2 Introduction

Group theory is the study of groups. Groups are sets equipped with an operation (like multiplication, addition, or composition) that satisfies certain basic properties. As the building blocks of abstract algebra, groups are so general and fundamental that they arise in nearly every branch of mathematics and the sciences. For example:

Symmetry groups appear in the study of combinatorics overview and algebraic number theory, as well as physics and chemistry. For example, Burnside's lemma can be used to count combinatorial objects associated with symmetry groups.



The molecule CCl_4X has tetrahedral shape; its symmetry group has 24 elements. Chemists use symmetry groups to classify molecules and predict many of their chemical properties.

9.3 Group

Definition: A group is a set G together with an operation that takes two elements of G and combines them to produce a third element of G. The operation must also satisfy certain properties.

More formally, the group operation is a function $G \times G \to G$, which is denoted by $(x, y) \mapsto x * y$, satisfying the following properties (also known as the group axioms).

Group Axioms:

1. *Associativity:* For any $x, y, z \in G$, we have $(x * y) * z = x * (y * z)$.
2. *Identity:* There exists an $e \in G$ such that $e * x = x * e = x$ for any $x \in G$. We say that e is an identity element of G.
3. *Inverse:* For any $x \in G$, there exists a $y \in G$ such that $x * y = e = y * x$. We say that y is an inverse of x.

   Note that the definition of the operation as a function implies
4. *Closure:* For any $x, y \in G$, $x * y$ is also in G.

Many definitions include this as a fourth "axiom" for emphasis. One common construction of groups is as subsets H of a known group G, with the same operation as in G. In this case, closure is important to check: for a, b in H, $a * b$ is an element of G that may or may not lie in H.

Examples To specify a group, we have to state what the set is, along with the group operation. The following are common examples of groups:

1. $\mathbb{Z}$, the set of integers, with the group operation of addition.
2. $\mathbb{R}^{\times}$, the set of non-zero real numbers, with the group operation of multiplication.
3. $\mathbb{Z}_n$, the set of integers $\{0, 1, 2, 3 \dots\ n-1\}$ with group operation of addition modulo n.
4. $\mathbb{Z}_n^{\times}$, the set of integers $\{1 \leq a \leq n-1 : \gcd(a, n) = 1\}$, with group operation of multiplication modulo n
5. S_n, the set of bijective functions $[n] \longleftarrow [n]$, where $[n] = \{1, 2, 3 \dots, n\}$, with the group operation of function composition.

Checking the axioms explicitly for example 1, we see that:

1. **Closure:** The sum of two integers is an integer. (So addition is an operation on $\mathbb{Z}$).
2. **Associativity:** It is well known that addition of integers is indeed associative.
3. **Identity:** For all integers a, $0 + a = a + 0 = a$. So 0 is an identity element for $\mathbb{Z}$ under addition.
4. **Inverse:** For all integers a, $a + (-a) = (-a) + a = 0$. So $-a$ is an additive inverse for a.

9.4 Group Properties and Definitions

This section contains some basic properties and definitions of terms that are used to describe groups and their elements.

The asociativity condition implies that it makes sense to drop the parentheses altogether and speak of the product of n elements of G, $a_1 * a_2 * dots * a_n$, since it does not matter how the parentheses are arranged. When the operation is clear, this product is often written without the $*$ sign, as $a_1 a_2 a_3 \dots a_n$. However, the order of the elements matters, since it is generally not true that $xy = yx \ \forall\ xy \in G$.

Definition The group G is *abelian* if $\forall\ x, y \in G$, $xy = yx$.

Note that the first four groups in the examples above are abelian, but S_n is not abelian for $n \geq 3$ (see the worked examples below).

Definition: Let $x \in G$ be an element with an inverse y. For any $m \in \mathbb{Z}$ define

$$x^m = \begin{cases} x * x * x * \cdots * x \quad (m \text{ terms}) \quad \text{if } m > 0 \\ e \quad \text{if } m = 0 \quad \text{if } m = 0 \\ y * y * y * \cdots * y \quad (m \text{ terms}) \quad \text{if } m < 0 \end{cases} \tag{33}$$

It is routine, but rather tedious, to show that the exponential laws of integers similarly hold.

For any $g \in G$ and $m, n \in \mathbb{Z}$, we have $g^{m+n} = g^m g^n$ and $(g^m)^n = g^{mn}$

Since groups are sets with restrictions, it is natural to consider subsets of groups. If $H \subseteq G$ and for a group H and G is also a group. Then we call H a subgroup of G.

Definition:
The order of a finite group G is the number of elements in G, denoted by $|G|$.
The order of an element $g \in G$ is the smallest positive integer k such that $g^k = e_G$

It is useful to understand that we can usually describe a group without listing out all of its elements. This is because we generally start with a set of elements, and then apply the group operation to all pairs of elements until we cannot create any more distinct elements. If a set of such elements X (and their inverses) can be used with a group operation $*$ to create a group G, we say that G is generated by X. If the smallest such X is finite, then we say G is finitely generated. If the smallest such X consists of only one element, we say that G is cyclic. Some examples are as follows:

Examples:

1. $\mathbb{Z}$ is cyclic, since it is generated by 1. This is because $1+1 = 2$, $2+1 = 3$, and so on, generating all positive integers. Similarly, $(-1)+(-1) = -2$, $(-2)+(-1) = -3$, and so on, generating all negative integers (here, -1 is the inverse of 1). And of course, $(-1)+1 = 0$, giving us the identity. Therefore, we have generated all the elements of $\mathbb{Z}$ using one element. By the same reasoning, all $\mathbb{Z}_n$ are cyclic.
2. $\mathbb{Q}$ is not finitely generated.
3. $\mathbb{Z}_8^*$ is generated by the elements $\{3, 5, 7\}$. Note that all of these elements have order 2, and the group itself is the set of generators along with the identity.
4. The symmetric group S_n is generated by the set of all 2 cycles (transpositions) in S_n. This is proven by showing that every cycle $(n_1 n_2 \dots n_k)$ can be written as a product of transpositions $(n_1 n_2)(n_2 n_3) \dots (n_1 n_k)$

9.5 Homomorphisms

given two groups, $(G,)$ and (H, Δ), a group homomorphism from $(G,)$ to (H, Δ) is a function$h : GH$ such that for all u and v in G it holds that

$$h(u * v) = h(u) \cdot h(v) \tag{34}$$

where the group operation on the left hand side of the equation is that of G and on the right hand side that of H. From this property, one can deduce that h maps the identity element e_G of G to the identity element e_H of H,

$$h(e_G) = e_H \tag{35}$$

and it also maps inverses to inverses in the sense that

$$h(u^{-1}) = h(u)^{-1} \tag{36}$$

Inuition: The purpose of defining a group homomorphism is to create functions that preserve the algebraic structure. An equivalent definition of group homomorphism is: The function $h : GH$ is a group homomorphism if whenever
$a * b = c$ we have $h(a) \cdot h(b) = h(c)$
In other words the group H in some sense has a similar algebraic structure to G and the Homomorphism h preserves that.

Examples:

1. For each real number c, the formula $c(x+y) = cx+cy$ for all x and y in $\mathbb{R}$ says that the function $M_c : \mathbb{R} \to \mathbb{R}$ where $M_c(x) = cx$ is a group homomorphism.

2. For all real numbers x and y, $|xy| = |x||y|$. Therefore the absolute value function $f : \mathbb{R}^\times \to \mathbb{R}_{>0}$, given by $f(x) = |x|$, is a group homomorphism. (We exclude 0, even though it works in the formula, in order for the absolute value function to be a homomorphism on a group.)

3. . For $x \in \mathbb{R}^\times$, let $s(x)$ be its sign: $s(x) = 1$ for $x > 0$ and $s(x) = -1$ for $x < 0$. Then $s(xy) = s(x)s(y)$ for all x and y in $\mathbb{R}^\times$, so $s : \mathbb{R}^\times \to \pm 1$ is a homomorphism.

4. Fix an integer n. For all real numbers x and y, $(xy)^n = x^n y^n$, so the n-th power map $f : \mathbb{R}^\times \to \mathbb{R}^\times$, where $f(x) = x^n$, is a homomorphism.

5. Fix a nonzero real number a. Since $a^{m+n} = a^m a^n$ for all integers m and n the function $f : \mathbb{Z} \to \mathbb{R}^\times$ where $f(n) = a^n$ satisfies $f(m + n) = f(m)f(n)$ for all m and n, so f is a homomorphism from the (additive) group $\mathbb{Z}$ to the (multiplicative) group $\mathbb{R}^\times$.

9.6 Isomorphisms

In abstract algebra, we say that two mathematical objects are isomorphic if they have the same structure. An isomorphism is a mapping between two such objects which preserves the structure of the objects. Isomorphisms therefore naturally appear in group theory, and can be defined as follows:

Definition:
An *isomorphism* $\Phi : G \to H$ between two groups G and H (with group operator $*_G$ and $*_H$, respectively) is a mapping which satisfies the following conditions:

1. Φ is a bijection

2. For every $x, y \in G$, we have $\phi(x *_G y) = \phi(x) *_H \phi(y)$

Two groups G and H are isomorphic ($G \cong H$) $\iff$ there exists an isomorphism between them. From the definition, taking isomorphic groups $G \cong H$ with isomorphism $\phi : G \to H$, the following statements hold:

1. Isomorphism map identity elements to identity elements. This follows since $\phi(g) = h$ then $\phi(g) = \phi(g *_G e_G) = \phi(g) *_H \phi(e_G) = h *_H \phi(e_G)$. Giving us $\phi(e_G) = e_H$ by left multiplying by h^{-1} on the equality $h *_H \phi(e_G) = h *_H e_H$

2. Isomorphisms map inverses to inverses.That is, for $x \in G$, $\phi(x^{-1}) = \phi(x)^{-1}$.This follows since for $x \in G$, using the fact that isomorphisms send identities to identities, $\phi(e_G) = \phi(x *_G x^{-1}) = \phi(x) *_H \phi(x^{-1}) = e_H$. Left-multiplying by $\phi(x)^{-1}$ gives us the desired equality $\phi(x^{-1}) = \phi(x)^{-1}$.

3. $|G| = |H|$ since ϕ is a bijection.

4. The inverse of an isomorphism is an isomorphism, and a composition of isomorphisms is an isomorphism.

Isomorphisms are useful for classifying groups of the same order, as well as for identifying groups which are identical in structure, even if they appear in different contexts. Some examples involving isomorphisms are as follows:

- $\mathbb{Z}_4 \cong 2\mathbb{Z}_4$ where $2\mathbb{Z}_4 = \{0, 2, 4, 6\}$ whose operation is addition modulo 8,
- $\mathbb{Z}_4 \cong \mathbb{R}$, where $\mathbb{R}$ is group of plane rotational symmetries of the swastik symbol. $R = \{e, r, r^2, r^3\}$ where r is a rotation by $\frac{\pi}{2}$ about an axis perpendicuar to the plane containing the symbol through its center.
- $\mathbb{Z}_8^x \cong C$, where C is he group of plane symmetries of a chessboard. $C = \{e, r, q_1, q_2\}$ where r is a rotation by π about an axis perpendicular to the board through its center, and q_1, q_2 are reflections across plane perpendicular to the board passing through opposite corners of the board.

9.7 Products

We can take products of groups to create more groups. The most straightforward way of doing this is the direct product.

Definition:

The direct product $G \times H$ of groups G and H (with operations $*_G$ and $*_H$, respectively) is a group containing the elements $\{(g,h)|g \in G^H \in H\}$, where the group operation $*_{GH}$ is defined as

$$(g_1, h_1) *_{GH} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

It is easy to verify that $G \times H$ is a group, since the identity is (e_G, e_H), the inverse of (g,h) is (g^{-1}, h^{-1}), and associativity and closure can follow directly from the associativity and closure of G and H.

There is a useful theorem for showing that a group is isomorphic to a direct product (of its subgroups):

Theorem

Let G be a group with subgroups H and K, where $HK = GHK = G$ (that is, every $g \in G$ can be written as hk for some $h \in H$ and $k \in K$). In addition, suppose every element of H commutes with every element of K, and $H \cap K = \{e\}$. Then, $G \cong H \times K$.

Some examples of direct products are as follows:

Examples:

- $\mathbb{Z}_2 \times \mathbb{Z}_2$ is commonly called Klien's group or V_4, and consists of the elements $\{(0,0),(0,1),(1,0),(1,1)\}$. Note that $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_8^\times$, but $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.
- The n dimensional coordinate plane is essentially a direct product of $\mathbb{R} \times \mathbb{R} \cdots \times \mathbb{R}$ (n times).
- We have $\mathbb{Z}_{mn} \cong \mathbb{Z}P_m \times \mathbb{Z}_n$ if and only if m and n ae relatively prime. Note that this is equivalent to saying that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic.

9.8 Transformation Group

A transformation group G is a non-void set of mappings of a certain set X onto itself with the following properties:

1. The identical map is included in G
2. If $g_1 \in G$ and $g_2 \in G$ then $g_1 g_2 \in G$
3. If $g \in G$ then g^{-1} exists and belongs to G

Some examples of the transformation group are: **Examples:**

- One of the most important transformation groups is the symmetric group S_n on n elements. Fix a finite number n and a set S of n elements, $S = \{1,2,3,...,n\}$. Let G be the group of all permutations of S. That is to say, an element of G is a one-to-one correspondence of the set S to itself. This G satisfies the three axioms mentioned above since

  1. The composition of two one-to-one correspondences is another one-to-one correspondence.
  2. The identity function is a one-to-one correspondence.
  3. A one-to-one correspondence has an inverse which is a one-to-one correspondence.

  This group G of all permutations on a set of n elements is called the symmetric group on n elements, and it is denoted S_n. Note that there are $n!$ elements of S_n.

- The group of isometries of the Euclidean plane.

9.9 Permutation Group

9.9.1 Notation

In mathematics, a permutation group is a group G whose elements are permutations of a given set M and whose group operation is the composition of permutations in G (which are thought of as bijective functions from the set M to itself). The group of all permutations of a set M is the symmetric group of M, often written as $Sym(M)$. The term permutation group thus means a subgroup of the symmetric group. If $M = \{1, 2, ..., n\}$ then, $Sym(M)$, the symmetric group on n letters is usually denoted by S_n.

The way in which the elements of a permutation group permute the elements of the set is called its group action.

Since permutations are bijections of a set, they can be represented by Cauchy's two-line notation. This notation lists each of the elements of M in the first row, and for each element, its image under the permutation below it in the second row. If σ is a permutation of the set $M = \{x_1, x_2, \ldots, x_n\}$ then,

$$\sigma = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_n) \end{pmatrix}$$

For instance, a particular permutation of the set 1,2,3,4,5 can be written as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

this means that σ satisfies $\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 3$, and $\sigma(5) = 1$. The elements of M need not appear in any special order in the first row.

Permutations are also often written in cyclic notation (cyclic form) so that given the set $M = \{1, 2, 3, 4\}$, a permutation g of M with $g(1) = 2$, $g(2) = 4$, $g(4) = 1$ and $g(3) = 3$ will be written as $(1, 2, 4)(3)$, or more commonly, $(1, 2, 4)$ since 3 is left unchanged; if the objects are denoted by single letters or digits, commas and spaces can also be dispensed with, and we have a notation such as (124). The permutation written above in 2-line notation would be written in cyclic notation as $\sigma = (125)(34)$..

9.9.2 Composition of Permutations - The Group Product

The product of two permutations is defined as their composition as functions, so $\sigma \cdot \pi$ is the function that maps any element x of the set to $\sigma(\pi(x))$. Note that the rightmost permutation is applied to the argument first, because of the way function application is written. Some authors prefer the leftmost factor acting first, but to that end permutations must be written to the right of their argument, often as a superscript, so the permutation σ acting on the element x results in the image x^σ. With this convention, the product is given by $x^{\sigma \cdot \pi} = (x^\sigma)^\pi$. However, this gives a different rule for multiplying permutations. This convention is commonly used in the permutation group literature, but this article uses the convention where the rightmost permutation is applied first.

Since the composition of two bijections always gives another bijection, the product of two permutations is again a permutation. In two-line notation, the product of two permutations is obtained by rearranging the columns of the second (leftmost) permutation so that its first row is identical with the second row of the first (rightmost) permutation. The product can then be written as the first row of the first permutation over the second row of the modified second permutation. For example, given the permutations,

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$$

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

The product QP is

$$QP = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

The composition of permutations, when they are written in cyclic form, is obtained by juxtaposing the two permutations (with the second one written on the left) and then simplifying to a disjoint cycle form if desired. Thus, in cyclic notation the above product would be given by:

$$QP = (15)(24)\dot{(}1243) = (1435)$$

Since function composition is associative, so is the product operation on permutations: $(\sigma \cdot \pi) \cdot \rho = \sigma \cdot (\pi \cdot \rho)$.

9.9.3 Neutral Element or Identity Element

The identity permutation, which maps every element of the set to itself, is the neutral element for this product. In two-line notation, the identity is

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \tag{37}$$

In cyclic notation, $e = (1)(2)(3)...(n)$ which by convention is also denoted by just (1) or even ().

9.9.4 Inverse of a Permutation

Since bijections have inverses, so do permutations, and the inverse σ^{-1} of σ is again a permutation. Explicitly, whenever $\sigma(x) = y$ one also has $\sigma^{-1}(y) = x$. In two-line notation the inverse can be obtained by interchanging the two lines (and sorting the columns if one wishes the first line to be in a given order). For instance

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 5 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 4 & 3 & 1 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$

To obtain the inverse of a single cycle, we reverse the order of its elements. Thus,
$(125)^{-1} = (521) = (152)$

To obtain the inverse of a product of cycles, we first reverse the order of the cycles, and then we take the inverse of each as above. Thus,
$[(125)(34)]^{-1} = (34)^{-1}(125)^{-1} = (43)(521) = (34)(152)$

Having an associative product, an identity element, and inverses for all its elements, makes the set of all permutations of M into a group, $Sym(M)$; a permutation group.

9.9.5 Examples

Consider the following set G_1 of permutations of the set $M = \{1, 2, 3, 4\}$:

- $e = (1)(2)(3)(4) = (1)$ This is the identity, the trivial permutation which fixes each element.
- $a = (12)(3)(4) = (12)$ This permutation interchanges 1 and 2, and fixes 3 and 4.

9.10 Continuous Groups

If, for a group G, group multiplication and inversion are continuous mappings, then G is a continuous group. *Alternatively:* A group having continuous group operations is called a continuous group.

A continuous group is necessarily infinite, since an infinite group just has to contain an infinite number of elements. But some infinite groups, such as the integers or rationals, are not continuous groups.

In general, the elements of a continuous group may be labelled by a number of continuous variables. For instance, the group of rotations in three dimensions with a fixed point is labelled by three angles — two to define the direction in space of the axis of rotation through the fixed point, the third
to specify the angle of rotation.

For rotation groups, the range of the continuous variables is generally finite. An example of a continuous group with a variable of infinite range is the group of translations along a line by a distance x, where $\infty < x < \infty$.

The continuous variables labelling the group elements are generally taken to be real. The composition rules relating the labels of a product to the labels of its factors may be either simple or complicated.

Examples:

1. The group of unimodular, unitary 22 matrices is $SU(2)$. Each matrix has four complex entries, so eight real parameters are required to specify it. The condition of unitarity imposes four real restrictions (two real diagonal restrictions and one complex off-diagonal restriction) and the condition that the determinant be $+1$ imposes one more. There remain three independent real parameters. This is a three-parameter continuous group. The infinitesimal generators of the group are traceless, anti-Hermitian 22 matrices. The most general such matrix takes the form

$$\begin{pmatrix} ia & b+ic \\ -b+ic & -ia \end{pmatrix}$$
$$= a\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
$$= aX_1 + bX_2 + cX_3$$

   where X_1, X_2, X_3 generate the associated Lie algebra $su(2)$ (Discussed in next section)

2. The group of unimodular, orthogonal 3×3 matrices is $SO(3)$. Each matrix has nine real entries, but the condition of orthogonality imposes three diagonal and three (symmetric) off-diagonal conditions, so there are three independent real parameters. The set of orthogonal 3×3 matrices divides into two subsets - one of matrices with determinant -1, the other of matrices with determinant $+1$. The latter subset is relevant here, and constitutes a three-parameter continuous group. Near the identity, the condition of orthogonality is $(1 + \epsilon M)^{tr}(1 + \epsilon M) = 1$, where A^{tr} is the transpose of the matrix A and ϵ is an infinitesimal. To lowest order in infinitesimals, this becomes $M^{tr} = -M$, so the infinitesimal generators of the group are real, antisymmetric 3×3 matrices. The most general such matrix takes the form

$$\begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix}$$
$$= a\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$
$$= aY_1 + bY_2 + cY_3$$

   where Y_1, Y_2, Y_3 generate the associated Lie algebra $so(3)$

9.11 Lie Groups

9.11.1 Definition

A real Lie group is a group that is also a finite-dimensional real smooth manifold, in which the group operations of multiplication and inversion are smooth maps. Smoothness of the group multiplication

$$\mu : G \times G \to G \quad \mu(x, y) = xy$$

means that μ is a smooth mapping of the product manifold $G \times G$ into G. These two requirements can be combined to the single requirement that the mapping

$$(x, y) \mapsto x^{-1}y$$

be a smooth mapping of the product manifold into G.

9.11.2 Examples

1. The 2×2 real invertible matrices form a group under multiplication, denoted by $GL(2, R)$ or by $GL_2(R)$:

$$GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} det(A) = ad - bc \neq 0 \right\}$$

   This is a four-dimensional noncompact real Lie group; it is an open subset of $\mathbb{R}^4$. This group is disconnected; it has two connected components corresponding to the positive and negative values of the determinant.

2. The rotation matrices form a subgroup of $GL(2, R)$, denoted by $SO(2, R)$. It is a Lie group in its own right: specifically, a one-dimensional compact connected Lie group which is diffeomorphic to the circle. Using the rotation angle φ as a parameter, this group can be parametrized as follows:

$$SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} : \varphi \in \mathbb{R}/2\pi\mathbb{Z} \right\}$$

   Addition of the angles corresponds to multiplication of the elements of $SO_2(\mathbb{R})$, and taking the opposite angle corresponds to inversion. Thus both multiplication and inversion are differentiable maps.

3. The affine group of one dimension is a two-dimensional matrix Lie group, consisting of 2×2 real, upper-triangular matrices, with the first diagonal entry being positive and the second diagonal entry being 1. Thus, the group consists of matrices of the form

$$A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} a > 0, b \in \mathbb{R}$$

10 Introduction to Möbius Transformations

10.1 Affine Transformations

Let us briefly recall a few basic properties of the complex numbers. If $z \in \mathbb{C}$, then we can write $z = r(\cos\theta + i\sin\theta)$, where r is the modulus, $|z|$, of z and θ the argument, $arg(z)$, of z. We will denote the real and imaginary part of z by $Re(z)$ and $Im(z)$, respectively. We have the following five basic maps, which we will study in the following:

- $z \mapsto cz$, $c \in \mathbb{R}$, Scaling
- $z \mapsto z + A$, $A \in \mathbb{C}$, Translation
- $z \mapsto Az$, $A = e^{i\theta}$, Rotation
- $z \mapsto \bar{z}$, Complex Conjugation
- $z \mapsto 1/z$, Inversion

Definition: A direct affine transformation is a combination of $(1), (2)$ and (3), i.e. a map of the form $T(z) = Az + B$.

Lemma 10.1.1 The direct affine transformation $T(z) = Az + B$ is a translation if and only if $A = 1$. If $|A| = 1$, $A \neq 1$ then T is a rotation about $\frac{B}{1-A}$ by an angle $arg(A)$.

Proof If $A = 1$, then $T(z) = z + B$ is a translation. If $|A| = 1$ and $A \neq 1$, we let F be a fixed point of T, i.e. a point where $T(F) = F$. Then we have $F = AF + B$, which implies $F = \frac{B}{1-A}$. Now

$$\begin{aligned} T(z) - F &= \frac{Az - A^2z + B - BA - B}{1 - A} \\ &= \frac{Az - A^2z - BA}{1 - A} \\ &= \frac{Az(1 - A) - B}{1 - A} \\ &= A(z - F) \end{aligned}$$

This shows that if $|A| = 1$ and $A \neq 1$ then T is a rotation about F by an angle $arg(A)$. □

Lemma 10.1.2 A direct affine transformation preserves circles and lines.

Proof A direct affine transformation, $T(z) = Az + B$, where $|A| = 1$ is by Lemma 10.1.1 a rotation about $\frac{B}{1-A}$ which clearly preserves circles and lines. A direct affine transformation, $T(z) = Az + B$, where $|A| \neq 1$ can be written as $T(z) = r(A^{'}z + B^{'}0)$, where r is real and $|A^{'}| = 1$. Again by Lemma 10.1.1 this map is a rotation about $\frac{B^{'}}{1-A^{'}}$ scaled by r, which preserves circles and lines. □

Theorem 10.1.1 Affine Transformations are Conformal.

Proof Using Lemma 10.1.2 we see that all circles and lines are preserved as circles and lies and we can infer that Affine Transformations are also Conformal.

10.2 The Inverse Transformation

The map T, $T(z) = 1/z$ is called inversion. If $z \neq 0$ then there is a unique $w = 1/z$, so $T : \mathbb{C}/0 \to \mathbb{C}/0$ is a bijection. Our goal is to extend T to a homeomorphism, $T : \mathbb{C}_\infty \to \mathbb{C}_\infty$. Notice that $1/z = \frac{\bar{z}}{|z|^2}$, so T is the composition of the two maps $S(z) = z$ and $R(z) = \frac{z}{|z|^2}$. Furthermore we see that $arg(R(z)) = arg(z)$ and that $|R(z)| = 1/|z|$, so R is inversion in the unit circle.

Theorem 10.2.1 Let T denote the inversion. The map T takes circles and lines to circles and lines.

Proof Let $w = 1/z$ be the image of z under T. If $w = a + ib$ and $z = x + iy$ then we have $a = \frac{x}{x^2+y^2}$, $b = \frac{-y}{x^2+y^2}$, $x = \frac{a}{a^2+b^2}$ and $y = \frac{-b}{a^2+b^2}$. The equation:

$$A(x^2 + y^2) + Bx + Cy + D = 0$$

is a circle or, if $A = 0$, then a line. Using the expressions for x, y in terms of a, b and substituting it into the equation for the circle or line, we get that a, b satisfying

$$D(a^2 + b^2) + Ba - Cb + A = 0$$

which is the equation for a circle or a line. □

Theorem 10.2.2 The inversion $T : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is a conformal map.
Proof We can write the inverse transform as

$$\begin{aligned} w &= \frac{1}{z} \\ \text{where} \quad z &= x + iy \\ w &= \frac{1}{x + iy} \\ w &= \frac{1}{x + iy} \cdot \frac{x - iy}{x - iy} \\ w &= \frac{x - iy}{x^2 + y^2} \end{aligned}$$

The above form is an affine equation and from Theorem 10.1.1 we know that all affine transformations are conformal, hence the Inverse transformation is also conformal. □

10.3 Möbius Transformations

A Möbius transformation $f : C_\infty \to C_\infty$ is a map

$$f(z) = \frac{az + b}{cz + d} \quad a, b, c, d \in \mathbb{C} \quad \text{and} ad - bc \neq 0 \tag{38}$$

We have the following basic theorems about any Möbius transformation f:

Theorem 10.3.1 f can be expressed as a composition of Affine Transformations and Inversion Transformations.
Proof We write f as

$$f = \frac{az + b}{xz + d} = \frac{\frac{a}{c}(cz + d) - \frac{ad}{c} + b}{cz + d} = \frac{a}{c} + \frac{b - \frac{ad}{c}}{cz + d}$$

If we let w_1, w_2 and w_3 be the maps $w_1 = cz + d$, $w_2 = 1/w1$ and $w3 = (b - \frac{ad}{c})w_2 + \frac{a}{c}$, then $f = w_3 \circ w_2 \circ w_1$. Note that if $c = 0$, there is no inversion in the decomposition of f.

Theorem 10.3.2 f maps $\mathbb{C}_\infty$ one-to-one onto itself, and is continuous.
Proof If $z \neq -d/c$ and $w = az+b/cz+d$, then $z = -dw+b/cw-a$. So, at every point $z \in \mathbb{C}$, $z6 \neq -d/c$, f is well-defined, one-to-one, onto and continuous. We extend f to a map $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ by setting $f(\infty) = \infty$, if $c = 0$. If $c \neq 0$, then we set $f(d/c) = \infty$. One can check that this makes f continuous as a function $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$. The inverse of f is given by

$$f^{-1}(w) = \frac{-dw + b}{cw - a}$$

Again, if $c = 0$, we set $f^{-1}(\infty) = \infty$. If $c \neq 0$, then we set $f^{-1}(a/c) = \infty$. With these choices, one can check that $f^{-1} : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is continuous. In summary, $f : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is a homeomorphism.

Theorem 10.3.3 f maps Circles and Lines to Circles and Lines.
Proof Since we have shown that both affine transformations and inversions take circles and lines to circles and lines, it follows from Theorem 10.3.1 that f takes circles and lines to circles and lines. See Lemma 10.1.1.

Theorem 10.3.4 f is conformal.

Proof This also follows from Theorem 10.3.1. since we have shown that affine transformations and inversions are conformal, see Theorem 10.1.1 and Theorem 10.2.2.

Theorem 10.3.5 The Möbius Transformation

$$T(z) = \frac{az+b}{cz+d}$$

has the inverse transformation

$$T^{-1}(z) = \frac{-dz+b}{cz-a}$$

In particular, the inverse of a Möbius transformation is also a Möbius Transformation.

Theorem 10.3.6 A Composition of a Möbius Transformation with another Möbius Transformation results in another Möbius Transformation.

Proof Let there be two Möbius Transformations $M_1(z)$ and $M_2(z)$ where

$$M_1(z) = \frac{a_1 z + b_1}{c_1 z + d_1} \quad \text{and} \quad M_2(z) = \frac{a_2 z + b_2}{c_2 z + d_2}$$

Now, composing both these transformation functions, we get

$$\begin{aligned} M_1 \circ M_2(z) &= \frac{a_1(\frac{a_2 z+b_2}{c_2 z+d_2}) + b_1}{c_2(\frac{a_2 z+b_2}{c_1 z+d_2}) + d_1} \\ &= \frac{(a_1 a_2 + b_1 c_2)z + (a_1 b_2 + d_2 b_1)}{(a_2 c_1 + c_2 d_1)z + (b_2 c_1 + d_1 d_2)} \end{aligned}$$

Let $A = a_1 a_2 + b_1 c_2$, $B = a_1 b_2 + d_2 b_1$, $C = a_2 c_1 + c_2 d_1$ and $D = b_2 c_1 + d_1 d_2$. So, we get

$$M_1 \circ M_2(z) = \frac{Az+B}{Cz+D}$$

which is a Möbius Transformation. □

Theorem 10.3.7 Any Möbius Transformation $T : \mathbb{C}^+ \to \mathbb{C}^+$ Fixes $1, 2$ or all points of $\mathbb{C}^+$.

Proof To find ficxed points of $T(z) = az + b/cz + d$, we want to solve

$$\frac{az+b}{cz+d} = z$$

for z which gives the quadratic equation

$$cz^2 + (d-a)z - b = 0 \tag{39}$$

If $c \neq 0$, then equation (39) must have 1 or 2 solutions, and hence there are 1 or 2 fixed points in this case.

If $c = 0$ and $a \neq d$, then the transformation has the form $T(z) = az + b/d$ which fixes ∞. From equation (39) the point $z = b/d - a \neq \infty$ is also a fixed point. So we have 2 fixed points in this case.

If $c = 0$ and $a = d$, then the equation (39) reduces to $0 = -b$, so $b = 0$ and the transformation is the identity transformation $T(z) = (az + 0)/(0z + a)$. The transformation fixed every point. □

Theorem 10.3.8 - Fundamental Theorem of Mobius Transformations There is a unique Mobius Transformation taking any distinct three points from $\mathbb{C}^+$ to any three distinct points of $\mathbb{C}^+$.

Proof Suppose z_1, z_2, z_3 are distinct points in $\mathbb{C}^+$ and w_1, w_2, w_3 are also distinct points in $\mathbb{C}^+$. We have to show there exists a unique mobius transformation that maps $z_i \mapsto w_i$ for all $i = 1, 2, 3$. To start we show that there exists a map built from inversions, that maps $z_1 \mapsto 1, z_2 \mapsto 0, z_3 \mapsto \infty$. we do so in the case $z_3 \mapsto \infty$.

First invert about any circle centered at z_3. This takes z_3 to ∞ as desired. Points z_1 and z_2 no doubt get moved, say to $z_1^{'}$ and $z_2^{'}$ respectively, neither of which is ∞. Secondly we do a translation that takes $z_2^{'}$ to 0. Such a translation will keep ∞ fixed. and take $z_1^{'}$ to some new point $z_1^{''}$'in $\mathbb{C}$. Thirdly we will rotate and dailate about the origin which keeps the points at 0 and ∞ fixed but brings $z_2^{''}$ to 1. This process yields a composition of inversions that maps $z_1 \mapsto 1, z_2 \mapsto 0$ and $z_3 \mapsto \infty$.

However this composition involves an odd number of inversions, so it is not a Mobius Transformation. To make this a mobius transformation we do another transformation and take a reflection acros the real axis. This keeps 1,0 and ∞ fixed. Thus there is a mobius transformation taking any three distinct points to 0, 1 and ∞. For now we let T denote the mobius transformation that maps $z_1 \mapsto 1, z_2 \mapsto 0$ and $z_3 \mapsto \infty$.

Similarly, we can also contruct a mobius transformation, call it S that takes $w_1 \mapsto 1, w_2 \mapsto 0$ and $w_3 \mapsto \infty$.

If we let S^{-1} denote the inverse transformation of S, then the composition $s^{-1} \circ T$ is also a Mobius Transformation. Given this transfomation we obtain.

$$\begin{aligned} S^{-1} \circ T(z_1) &= S^{-1}(1) = w_1 \\ S^{-1} \circ T(z_2) &= S^{-1}(0) = w_2 \\ S^{-1} \circ T(z_3) &= S^{-1}(\infty) = w_3 \end{aligned}$$

Now, we have to prove that this mobius transformation for the given three points z_1, z_2 and z_3 is unique, we will use the method of contradiction. Assume that there are 2 transformations U and V that map $z_1 \mapsto w_1, z_2 \mapsto w_2$ and $z_3 \mapsto w_3$. Then $V^{-1} \circ U$ is a mobius Transformation that fixes more than 2 points, and this is an identity transformation. Thus $V^{-1} \circ U(z) = z$ for all $z \in \mathbb{C}^+$. Similarly $U \circ V^{-1}(z) = z$, and it follows that $U(z) = V(z)$ for all $z \in \mathbb{C}^+$. That is U and V are the same map. $\square$

Definition The *cross ratio* of 4 complex numbers z, w, u and v, where w, u and v are distinct is denoted by $(z, w; u, v)$ and

$$(z, w; u, v) = \frac{z-u}{z-v} \cdot \frac{w-v}{w-u} \tag{40}$$

If z is a variable and u, v, w are distinct complex constants then $T(z) = (z, w; u, v)$ is the *unique* Mobius Transformation that sends $w \mapsto 1, u \mapsto 0$ and $v \mapsto \infty$.

Example Find $T(z) = (z, 1; i, 2)$

$$\begin{aligned} T(z) = (z, 1; i, 2) &= \frac{z-i}{z-2} \cdot \frac{1-2}{1-i} \\ &= \frac{-z+i}{(1-i)z-2+2i} \end{aligned}$$

Theorem 10.3.9 - Invariance of Cross Ratio Suppose z_0, z_1, z_2 and z_3 are four distinct points in $\mathbb{C}^+$ and T is any mobius transformation. Then

$$(z_0, z_1; z_2, z_3) = (T(z_0), T(z_1); T(z_2), T(z_3))$$

Proof Let T be an arbitrary Mobius Transformation, and define $S(z) = (z_0, z_1; z_2, z_3)$, which sends $z_1 \mapsto 1, z_2 \mapsto 0, z_3 \mapsto \infty$. Notice that the composition of $S \circ T^{-1}$ is a mobius transformation that sends $T(z_1) \mapsto 1, T(z_2) \mapsto 0$ and $T(z_3) \mapsto \infty$. So this map can be expressed in the cross ratio as

$$S \circ T^{-1}(z) = (z, T(z_1); T(z_2), T(z_3))$$

Plugging $T(z_0)$ into this transformation we get

$$S \circ T^{-1}(z_0) = (T(z_0), T(z_1); T(z_2), T(z_3))$$

On the other hand $S \circ T^{-1}(T(z_0)) = S(z_0)$ which equals $(z_0, z_1; z_2, z_3)$. So, we have proved that

$$(z_0, z_1; z_2, z_3) = (T(z_0), T(z_1); T(z_2), T(z_3))$$

Theorem 10.3.10 Given any 2 clines C_1 and C_2, there exists a Mobius Transformation T that maps C_1 and C_2. That is $T(C_1) = C_2$.

Proof Let p_1 be a point on C_1 and q_1 and q_1^* be symmetric with respect to C_1. Similarly let p_2 be a point on C_2 and let q_2 and q_2^* be symmetric to C_2. Build the Mobius Transformation that send $p_1 \mapsto p_2$, $q_1 \mapsto q_2$ and $q_1^* \mapsto q_2^*$. Then $T(C_1) = C_2$.

10.4 Normal Form - 2 Fixed Points in Mobius Transformations

Suppose $T(z) = az + b/cz + d$ is a Mobius Transformation that fixes 0 and ∞. In this case, the form of the Mobius Transformation can be simplified. In particular that fixes 0 and ∞. In this case the form of the Mobius Transformation can be simplified. In particular, since $T(0) = 0$, it follows that $b = 0$. And since $t(\infty) = \infty$, it follows that $c = 0$. Thus $T(z) = \frac{a}{d}z$ which may be written as

$$T(z) = re^{i\theta}z$$

With T in this form it is clear that T fixes 0 and ∞, then T is a combination of a dilation (by factor r) and a rotation about the origin (by factor θ). We may assume that $r > 0$ in the above equation, because if it is negative, we can turn we can turn it into a positive constant by adding π to the angle of rotation.

A dilation with r will push points along lines through the origin. All points in the plane are headed towards ∞ (if $r > 1$) or towards 0 (if $0 < r < 1$) or there is no dilation if $r = 1$.

Now assume that T is a mobius transformation that fixes two finite points p and q (neither is ∞). Let

$$S(z) = \frac{z - p}{z - q}$$

be a Mobius Transformation that takes p to 0 and q to ∞. Let U be a Mobius Transformation determined by the composition

$$U = S \circ T \circ S^{-1}$$

Notice

$$U(0) = S \circ T \circ S^{-1}(0) = S \circ T(p) = S(p) = 0$$
$$U(\infty) = S \circ T \circ S^{-1}(\infty) = S \circ T(q) = S(q) = \infty$$

That is, U is a mobius Transformation that fixes 0 and ∞. So U is a combination of a rotation, dilation and can be expressed as $U = re^{i\theta}z$. Re-writing the equation of T using U as $S \circ T = U \circ S$. We arrive at the normal form with 2 fixed points.

$$\frac{T(z) - p}{T(z) - q} = re^{i\theta}\frac{z - p}{z - q} \tag{41}$$

Lemma 10.4.1 Suppose T is a Mobius Transformation that fixes to distinct finite points p and q, sends z_∞ to ∞, and sends ∞ to w_∞. Then $p + q = z_\infty + w_\infty$.

Proof Suppose T satisfies the condition of the Lemma. Then T has the normal form

$$\frac{z - p}{z - q} = \lambda\frac{T(z) - p}{T(z) - q}$$

where $\lambda = re^{i\theta}$. Plugging in $z = z_\infty$ in the normal form to see

$$\frac{z_\infty - p}{z_\infty - q} = \lambda \cdot 1$$

Pluging in $z = \infty$ into the normal form to see

$$1 = \lambda \frac{w_\infty - p}{w_\infty - q}$$

Solving the above to equations to obtain

$$\begin{aligned} \frac{z_\infty - p}{z_\infty - q} &= \frac{w_\infty - q}{w_\infty - p} \\ (z_\infty - p)(w_\infty - p) &= (w_\infty - q)(z_\infty - q) \\ (p - q)(p + q) &= (p - q)(z_\infty + w_\infty) \\ p + q &= z_\infty + w_\infty \end{aligned}$$

Theorem 10.4.1 If T is a mobius Transformation that fixes two distinct, finite points p and q, sends z_∞ to ∞ and sends ∞ to w_∞, then

$$T(z) = \frac{w_\infty z - pq}{z - z_\infty}$$

Proof In the proof of Lemma 10.4.1 we found that the constant λ in the normal form of T is

$$\lambda = \frac{z_\infty - p}{z_\infty - q} \tag{42}$$

It follows that T has the normal form

$$\frac{z - p}{z - q} = \frac{z_\infty - p}{z_\infty - q} \cdot \frac{T(z) - p}{T(z) - q}$$

Solving the expression for $T(z)$ and reducing using that fact that $p + q = z_\infty + w_\infty$, we get the desired result. □

10.5 General Linear Group ($\mathbf{GL}_n(\mathbb{R})$ or $\mathbf{GL}_n(\mathbb{C})$)

The general linear group of degree n is the set of nn invertible matrices, together with the operation of ordinary matrix multiplication. This forms a group, because the product of two invertible matrices is again invertible, and the inverse of an invertible matrix is invertible, with identity matrix as the identity element of the group. The group is so named because the columns of an invertible matrix are linearly independent, hence the vectors/points they define are in general linear position, and matrices in the general linear group take points in general linear position to points in general linear position.

10.6 Fractional Linear Transformations

Definition We let $\mathrm{GL}_2(\mathbb{C})$ be the set of invertible 2×2 matrices,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with complex entries, i.e $a, b, c, d \in \mathbb{C}$. Note that the identity Matrix

$$I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{is in} \quad \mathrm{GL}_2(\mathbb{C})$$

1. If $A, B \in \mathrm{GL}_2(\mathbb{C})$, then $AB \in \mathrm{GL}_2(\mathbb{C})$
2. If $A \in \mathrm{GL}_2(\mathbb{C})$ then,

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad \text{is in } \mathrm{GL}_2(\mathbb{C})$$

A transformation of the form

$$w = f(z) = \frac{az + b}{cz + d} \tag{43}$$

where $a, b, c, d \in \mathbb{C}$ and $ad - bc \neq 0$ is a conformal mapping called a Linear Fractional Transformation. The Transformation can be extended to the entire complex plane $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ by defining

$$f(-\frac{d}{c}) = \infty$$
$$f(\infty) = \frac{a}{c}$$

The linear fractional transformation is linear in both w and z, and analytic everywhere except a simple pole at $z = -d/c$.

Every linear fractional transformation except $f(z) = z$ has one or two fixed points. The linear fractional transformation sends circles and lines to circles or lines. Linear fractional transformations preserve symmetry. The cross ratio is invariant under a linear fractional transformation. A linear fractional transformation is a composition of translations, rotations, magnifications, and inversions.

The fractional linear transformation can be composed using the General Linear Group ($\mathrm{GL}_2(\mathbb{C})$) such as

$$g : z \mapsto g \cdot z = \frac{az + b}{cz + d} \tag{44}$$

where

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, x \in \mathbb{R}$$

10.7 Projective Linear Transformations ($\mathbf{PGL}_2(\mathbb{C})$)

The Projective linear group or the Projective General Linear Group is the induced action of the general linear group of a vector space V on the associated Projective space $P(V)$.

Explicitly the Projective Linear group is the quotient group.

$$PGL(V) = GL(V)/Z(V) \tag{45}$$

Where $GL(V)$ is the general linear group and $Z(V)$ is the subgroup of all non-zero scalar transformations of V. These are quotiented out because they are trivally on the projective space and they form the kernel of the action, and the notation Z reflects the scalar transformation at the center of the general linear group.

11 Solved Examples from Geometry of Möbius Transformations by Vladmir. V. Kisil

11.1 Chapter 1: Erlangen Programme: Preview

The Erlangen program is a method of characterizing geometries based on group theory and projective geometry. It was published by Felix Klein in 1872 as Vergleichende Betrachtungen über neuere geometrische Forschungen. It is named after the University Erlangen-Nürnberg, where Klein worked.

By 1872, non-Euclidean geometries had emerged, but without a way to determine their hierarchy and relationships. Klein's method was fundamentally innovative in three ways:

- Projective geometry was emphasized as the unifying frame for all other geometries considered by him. In particular, Euclidean geometry was more restrictive than affine geometry, which in turn is more restrictive than projective geometry.
- Klein proposed that group theory, a branch of mathematics that uses algebraic methods to abstract the idea of symmetry, was the most useful way of organizing geometrical knowledge; at the time it had already been introduced into the theory of equations in the form of Galois theory.
- Klein made much more explicit the idea that each geometrical language had its own, appropriate concepts, thus for example projective geometry rightly talked about conic sections, but not about circles or angles because those notions were not invariant under projective transformations (something familiar in geometrical perspective). The way the multiple languages of geometry then came back together could be explained by the way subgroups of a symmetry group related to each other.

11.2 Chapter 2: Groups and Homogenous Spaces

Definition 11.2.1 A *transformation group* G is a non-void set of mappings of a certain set X into itself with the following properties:

1. The identical map is included in G.
2. If $g_1 \in G$ and $g_2 \in G$ then $g_1 g_2 \in G$.
3. If $g \in G$ then g^{-1} exists and belongs to G.

Question 11.2.1 List all transformation groups on a set of three elements.
Solution Let $\Phi : G \to S_3$ be an abelian group where S_3 represents all permutations on a set of 3 elements. Now, the possible transformation groups are:

1. S_3
2. 3 Cyclic Groups
3. 3 Reflective Groups
4. Identity Group (I)

So, there will be 8 groups in total.

Question 11.2.2 Verify that the group of permutations of n elements are Transformation Groups.
Solution To prove that the Permutation group is a transformation group, we must show that the permutation group satisfies the 3 properties of a group which are:

1. There exists an identity element for the group G.
2. If $g_1 G$ and $g_2 \in G$ then $g_1 \cdot g_2 \in G$

3. If $g \in G$ then $g^{-1} \in G$. That is there is an inverse element for every element in G

We can see that there is an identity element for every permutation group S_n of n elements using Section 9.9.3 and equation (37). We can also see that there exists an inverse for every element in the permutation group in section 9.9.4. We can see that the composition of any 2 elements of the permutation group of size n is also a permutation group using sub-section 9.9.2 - The Group Product inside permutation groups. Hence the permutation group of size n is a Transformation group. □

Question 11.2.3 Verify that the group of rotations in the unit circle T are Transformation Groups.

Solution Let us denote a rotation in the unit circle as R_α where α represents the angle in radians that we have rotated the object by in anti-clockwise direction. We can also state that for any 2 rotations R_α and R_β (where α and β are the angles of rotation), the composition $R_\alpha \circ R_\beta$ denotes the combined rotation denoted by$R_{\alpha+\beta}$.

Hence for all $R_\alpha, R_\beta \in G$, $R_\alpha \circ R_\beta = R_{\alpha+\beta} \in G$. Also there exists an identity element R_0 (rotation by zero radians), such that $R_\alpha \circ R_0 = R_0 \circ R_\alpha = R_\alpha$.

There also exists an inverse for every $R_\alpha \in G$, $R_{-\alpha}$ such that $R_\alpha \circ R_{-\alpha} = R_0$.

Hence the transformation in the unit plane constitutes a transformation group. □

Question 10.2.4 Verify that the group of shifts in the real line $\mathbb{R}$ are Transformation Groups.

Solution Let the shift of any point in the 2 dimensional cartesian coordinate be denoted by

$$\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

Where u, v denote the new coordinate values of the transposed x, y coordinates after translating them by a factor of a and b. Now to denote the real line - $\mathbb{R}$, we will take $y = 0$, which transform the above transformation matrix as:

$$\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ 0 \\ 1 \end{bmatrix}$$

Now, we can represent a shift S by the matrix

$$S = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \quad \forall \ a, b \in \mathbb{R}$$

Now I is the identity element where

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

such that

$$\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x \\ 0 \\ 1 \end{bmatrix}$$

Hence, there exists an identity element.

Now let us take to shift matrices denoted by S_1 and S_2, such that

$$S_1 = \begin{bmatrix} 1 & 0 & a_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{bmatrix} \quad \textbf{and} \quad S_2 = \begin{bmatrix} 1 & 0 & a_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{bmatrix}$$

Applying both of these transformations as $S_1 \circ S_2$, we get

$$S_1 \circ S_2 = \begin{bmatrix} 1 & 0 & a_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & a_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_1 + a_2 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{bmatrix}$$

We can clearly see that $S_1 \circ S_2 \in G \ \forall \ S_1, S_2 \in G$.

Now we can also see there exists an inverse for every transformation $S \in G$, such that

$$S^{-1} = \begin{bmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix}$$

, such that

$$S \circ S^{-1} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

Hence, there also exists an inverse $\forall S \in G$. The Translation of the real line $\mathbb{R}$ satisfies all three conditions and hence is a transformation group. □

Question 11.2.4 Verify that the group of shifts of the plane $\mathbb{R}^2$ is a transformation group.

Solution A shift of any 3D coordinate in the euclidean space denoted by (x, y, z) to the new coordinates (u, v, w) can be denoted by:

$$\begin{bmatrix} u \\ v \\ w \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ 1 \end{bmatrix}$$

where $a, b, c \in \mathbb{R}$ and denote the translation co-efficient in the three axes. Now for the plane $\mathbb{R}^2$, we can denote that by substituting $z = 0$, and obtaining:

$$\begin{bmatrix} u \\ v \\ w \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 0 \\ 1 \end{bmatrix}$$

, where

$$S = \begin{bmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

denotes the transformation matrix and is an element of the set of all shifts of the plane $\mathbb{R}^2$.

Now, we can show that there exists an identity element I

$$\grave{I} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

such that

$$\begin{bmatrix} u \\ v \\ w \\ 1 \end{bmatrix} = I \cdot \begin{bmatrix} x \\ y \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x \\ y \\ 0 \\ 1 \end{bmatrix}$$

Hence, there is an identity element I in the set of all shifts of the plane $\mathbb{R}^2$.

Now, let us take two shifts in the plane $\mathbb{R}^2$ denoted by S_1 and S_2 such that

$$S_1 = \begin{bmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & b_1 \\ 0 & 0 & 1 & c_1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad S_2 = \begin{bmatrix} 1 & 0 & 0 & a_2 \\ 0 & 1 & 0 & b_2 \\ 0 & 0 & 1 & c_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

such that all $a_i, b_i, c_i \in \mathbb{R} \ \forall \ i \in \{1, 2\}$ and $S_1, S_2 \in G$. Now applying the group operation (applying both shifts successively to the plane $\mathbb{R}^2$) which is matrix multiplication in this case, we get:

$$S_1 \circ S_2 = \begin{bmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & b_1 \\ 0 & 0 & 1 & c_1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 0 & a_2 \\ 0 & 1 & 0 & b_2 \\ 0 & 0 & 1 & c_2 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & a_1 + b_1 \\ 0 & 1 & 0 & b_1 + b_2 \\ 0 & 0 & 1 & c_1 + c_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

We can clearly see that $S_1 \circ_2 \in G \ \forall S_1, S_2 \in G$.

Next, we can also show that there exists an inverse element for each $S \in G$, denoted by:

$$S^{-1} = \begin{bmatrix} 1 & 0 & 0 & -a \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & -c \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

such that, $S \circ S^{-1} = S^{-1} \circ S = I$, as we can see below

$$S \circ S^{-1} = \begin{bmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & -a \\ 0 & 1 & 0 & -b \\ 0 & 0 & 1 & -c \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I = S^{-1} \circ S$$

Hence there also exists an inverse for every element $S \in G$, and as this set G satisfies all three conditions, this is a transformation group. □

In general all translations and shifts of the field $\mathbb{R}^n$ represents a transformation group and this result can be extended by using the above method for any matrix of $n \times n$ size and can also be generalized that the group $\mathrm{GL}_n(\mathbb{R})$ represents the translation group and is a translation group.

Question 11.2.5 Verify that the group of one-to-one linear maps of an n-dimensional vector space over a field $\mathbb{F}$ onto itself.

Solution Let us represent V as an n-dimensional vector space as

$$B = \{v_1, v_2, v_3 \dots v_n\} \tag{46}$$

where each $\{v_i\}$ is a vector in V.

Define a map $T :\to \mathbb{F}^n$ by sending each vector $v \in V$ to it's coordinate vector $[v]_B$ with respect to its basis B. The coordinate vector v in terms of of its basis B can be dented as:

$$[v]_B = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} c_1 c_2 c_3 \dots c_n \end{bmatrix}^T \tag{47}$$

where $c_i \in \mathbb{R}$.

Now, let us define the group operation $\cdot$ as $+$, so there exists an identity element I such that

$$I = \begin{bmatrix} 000 \cdot 0 \end{bmatrix}^T$$

and we can also show that for any vector $v \in V$

$$v + v_0 = [v]_B + v_0 = \begin{bmatrix} c_1 c_2 c_3 \cdots c_n \end{bmatrix}^T + \begin{bmatrix} 000 \cdots 0 \end{bmatrix}^T = \begin{bmatrix} c_1 c_2 c_3 \cdots c_n \end{bmatrix}^T = [v]_B = v$$

Hence there exists an identity element (also called the zero vector) where $v_0 = I \in V$.

Now, we can also show that there exists an inverse $v^{-1} \in V$ for all $v \in V$. Such that:

$$v^{-1} = \begin{bmatrix} -c_1 & -c_2 & -c_3 & \cdots & -c_n \end{bmatrix}^T$$

where

$$v + v^{-1} = \begin{bmatrix} c_1 & c_2 & c_3 & \cdots & c_n \end{bmatrix}^T + \begin{bmatrix} -c_1 & -c_2 & -c_3 & \cdots & -c_n \end{bmatrix}^T = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \end{bmatrix}^T = v_0 = I$$

Hence there also exists an inverse element for all $v \in V$.

Now, we ca also sow that for any two vectors $\alpha, \beta \in V$, the vector $\alpha + \beta \in V$. Let $\alpha = [a_i]_B$ and $\beta = [b_i]_B$ where where $i \in \{0, 1, 2 \cdots n-1\}$ and $a_i, b_i \in \mathbb{R}$. Now $\alpha + \beta = [a_i + b_i]_B$ which clearly $\in V$, hence all the three conditions are satisfied and the one-to-one linear maps over field $\mathbb{F}$ are a transformation group. □

Question 11.2.6 Verify that the group of Linear Fractional Mobius Transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d}$$

of the extended complex plane such that $ad - bc \neq 0$ represents a transformation group.

Solution Now, we can define an identity element I such as

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : z \mapsto \frac{z + 0}{0 + 1} = z$$

We can also compose with some linear-fractional transformation with the identity element to see that:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Note: We can also observe that there exist multiple identity element for the mobius Transformation of the form kI, such that:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} = k \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$k \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{akz + bk}{ckz + dk} = \frac{az + b}{cz + d} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z$$

Now, we will show that the composition of multiple linear fractional transformations (or mobius transformations) also results in another linear fractal transformation, which has also been stated in Theorem 10.3.6 under Section 10.3 - Mobius Transformations.

Let there be two linear-fractional transformations represented by M_1 and M_2 where

$$M_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

$$M_1 \circ M_2 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \circ \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}$$

We can clearly see that this composition is also a linear fractional transformation, and hence for any $M_1, M_2 \in G$, $M_1 \circ M_2 \in G$.

Now, we will state the inverse for every element $M \in G$. As a linear-fractional transformation is simply a 2×2 matrix, we can find the inverse if the determinant is not 0. It is given that for all mobius transformations $ad - bc \neq 0$ i.e. $|M| = ad - bc \neq 0$, hence the determinant is also not 0 and inverse must exist. The inverse is defined as:

$$M^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

As the linear-fractional transformation exists for all $a, bc, d \in \mathbb{C}_\infty$ we state that it is a transformation group. □

Question 11.2.7 Prove that any Transformation group is also an Abstract Group (Simply Group).
Solution The transformation group G of non-void set mappings satisfies the following properties:

1. The identical map is included in G, i.e. has an identity element $I \in G$.
2. If $g_1 \in G$ and $g_2 \in G$, then $g_1 \circ g_2 \in G$.
3. If $g \in G$, then g^{-1} exists and belongs to G.

We also know that an abstract group (or simply group) is a non-void set G on which there is a law of group multiplication (i.e. mapping $G \times G \to G$) with the properties:

1. Associativity: $g_1(g_2g_3) = (g_1g_2)g_3$
2. The existence of the Identity: $e \in G$ such that $eg = ge = g$ for all $g \in G$.
3. There existence of an inverse: for every $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.

If we have a transformation group then using the definition we can postulate that there must be an inverse and hence the third property of the abstract Group is satisfied.

We can also see that in a transformation group there must exist an identity element and hence the second property of the abstract group is also satisfied.

It is given in the definition of the abstract group that the group is formed using a binary operation $\circ$ which is group multiplication, but we also know that multiplication is inherently an associative property, so the first property of the abstract group is also inherently fulfilled by the definition of the abstract group.

Hence, we can state that all Transformation groups are abstract groups. □

Question 11.2.8 Verify that the group of isometric mappings of an equilateral triangle onto itself is an Abstract Group.
Solution To prove that a relation is a grup, we need t prove the following 3 axioms:

1. Associativity: $g_1(g_2g_3) = (g_1g_2)g_3$
2. The existence of the Identity: $e \in G$ such that $eg = ge = g$ for all $g \in G$.
3. There existence of an inverse: for every $g \in G$ there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.

Now, a isometric mapping is a mapping is a mapping that preserves lengths. So, an isometric mapping of an equilateral triangle onto itself basically implies that an equilateral triangle is being transformed on the real plane $\mathbb{R}^2$ using either rotation or translation, but no scaling as he lengths of the sides of the triangle are maintained.

We can depict any transformation on the real plane of any coordinate (x, y) to the new coordinate (u, v) using the composition of of a translation matrix M and a rotation matrix R deoted as:

$$T = M \cdot R = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \\ 0 & 0 & 1 \end{bmatrix}$$

where T is the transformation matrix and $a, b, \theta \in \mathbb{R}$ where a is the translation in $X - axis$, b the translation in the Y - axis and θ is the angle of rotation.
We can denote the transformed coordinates (x, y) into (u, v) as:

$$\begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = T \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}$$

Now, let us take 3 consecutive transformations as Transformation matrices as T_1, T_2 and T_3. We can clearly see using associative property of matrix multiplication that $T_1(T_2T_3) = (T_1T_2)T_3$, hence this satisfies associativity.

We ca also see that there exists an identity element I, such that

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

such that any transformation $T \in G$, implies $T \cdot I = I \cdot T = T$.

We can also see that there exists an inverse for every transformation $T \in G$, such that

$$T^{-1} = \begin{bmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \\ 0 & 0 & 1 \end{bmatrix}$$

such that $T \cdot T^{-1} = T^{-1} \cdot T = I$. hence the set of all isometric mappings of an equilateral triangle to itself satisfies all axioms of an abstract group and is hence a group. □

Question 11.2.9 Verify that the group of all permutations of a set of free elements is an Abstract Group.

Solution We have verified in Question 11.2.2 that the set of permutations of n elements is an abstract group, and we have also proved in Question 10.2.7 that transformation groups are abstract groups, hence using the above 2 proofs we can clearly state that all Permutation groups of n elements denoted by S_n is a group. □

Question 11.2.10 Verify that the group of invertible matrices of order 2 with coefficients in the field of integers modulo 2 is an Abstract Group.

Solution Any 2×2 matrix in the field of Integers modulo 2 ($\mathbb{Z}_2$) can be denoted as:

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where $a, b, c, d \in \mathbb{Z}_2 = \{0, 1\}$ and it is also given that this matrix is invertible i.e. $ad - bc \neq 0$. Now, we know that matrix multiplication is associative hence the first property is satisfied. We can also show that there exists an inverse:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

such that for any matrix $m \in G$, we have $m \cdot I = I \cdot m = m$. Hence hence is also an identity element that exists.

We can also see the for every element $M \in G$, there exists as inverse as the question clearly states all *invertible* matrices. Hence the set of all invertible matrices of $2 \times 2 \in \mathbb{Z}_2$ is an abstract group. □

Question 11.2.11 Verify that the group of linear fractional transformations of the extended complex plane generated by the mapping $z \to z^{-1}$ is an Abstract Group.

Solution We know that multiplication is an associative property and for any three transformations of z_1, z_2 and z_3, we can clearly state that:

$$\frac{1}{z_1}\left(\frac{1}{z_2}\frac{1}{z_3}\right) = \left(\frac{1}{z_1}\frac{1}{z_2}\right)\frac{1}{z_3}$$

Hence the first property of a group is satisfied.

Now, we can also state that there exists an identity element, namely $I = 1$, such that $g\cdot = 1 \cdot g = g \ \forall g \in G$. Hence it also satisfies the second condition of a group.

Now, we state the inverse for every $g \in G$, which can be denoted by $g^{-1} = 1/g$, such that

$$g \cdot \frac{1}{g} = \frac{1}{g} \cdot g = 1 = I$$

hence there also exists an inverse for every $g \in G$. Now for $g = 0$, the inverse would be ∞ and we define $\frac{1}{\infty} = 0$ and ∞ is also defined in the extended complex plane, hence under the extended complex plane all 3 axioms of a group are satisfied,

hence the transformation of $z \to z^{-1}$ is a group. □

Question 11.2.12 Verify that the group of linear fractional transformations of the extended complex plane generated by the mapping $z \to 1 - z$ is an Abstract Group.

Solution The linear fractional transformation $z \to 1-z$ can abe denoted as a special case of the Mobius Transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

where $a = -1, b = 1, c = 0$ and $d = 1$ and $|M| = ad - bc = -1$. Hence this is an invertible matrix an if we can prove that the linear-fractional Mobius transformation over the set of extended complex plane ($\mathbb{C}_\infty$) is a group, then by extension $z \to z^{-1}$ and $z \to 1 - z$ will also be abstract groups.

The set of linear-fractional Mobius Transformations is associative by Matrix multiplication, and hence satisfies the first property of an abstract group.

We can also see that there is an identity element I for every $g \in G$ where G is the set of all linear-fractional Mobius transformations such that $I \cdot g = g \cdot I = g$, where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Hence the set of linear-fraction Mobius Transformations also satisfies the second property of an abstract group.

We can also see that there exists an inverse for every $g \in G$ where $g^{-1} \cdot g = g \cdot g^{-1} = I$ such that:

$$g^{-1} = \frac{1}{|g|}(Adj(g))^T$$

where $|g|$ represents the non-zero determinant and $Adj(g)$ represents the Adjoint of the 2×2 matrix. Hence the set of linear-fractional mobius transformations also satisfies the third property and is hence an abstract group. By extension it can be shown that the transformation under the extended complex plane $z \to 1 - z$ is also an abstract group. □

Question 11.2.13 Show that a continuous group is locally compact if there exists a compact neighbourhood of its identity.

Solution The question can also be rephrased as: Let G_1 and G_2 be topological groups. Show that a homomorphism $h; G_1 \to G_2$ is continuous if and only if it is continuous at the identity $e \in G$.

One direction is trivial, namely, if h is continuous then obviously continuous at $e \in G_1$. Now for the reverse direction. Assume h is continuous at e. Choose some open set $U \subset G_2$. We want to show that its pre-image under h is also open. If $h^{-1}(U) = \phi$ we are done. If not then choose some $f(x) \in U$ with $x \in G_1$. We have that:

$$h^{-1}(U) = xh^{-1}(U_e)$$

where $U_e = h(x^{-1})U$. To see this we observe the following sequences of equivalences:

$$\begin{aligned} m \in h^{-1}(U) &\iff h(m) \in U \\ &\iff h(x^{-1}m) = h(x^{-1})h(m) \in h(x^{-1})U = U_e \\ &\iff x^{-1}m \in h^{-1}(U_e) \\ &\iff m \in xh^{-1}(U_e) \end{aligned}$$

Hence $h^{-1}(U) = xh^{-1}(U_e)$. Since translation functions on topological groups are homeomorphisms we have that U_e is open and G_2 and contains $h(e) = e_{G_2}$. Hence $h^{-1}(U_e)$ is open in G_1 by hypothesis. Thus $xh^{-1}(U_e) = h^{-1}(U)$ is open and that proves that the continuous group is locally compact if there exists a compact neighbourhood of its identity. □

Definition 12.2.2 A *subgroup* of a group G is a subset $H \subset G$ such that the restriction of multiplication from G to H makes H a group itself.

Question 12.2.14 Show that the $ax + b$ group is a subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Solution We have to show that the group $ax + b$ created by all dilations and translations of the real line is a subgroup to the group of all real 2×2 matrices with determinant 1 of the form:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{ax+b}{cx+d}$$

such that $a, b, c, d \in \mathbb{R}$ and $ad - bc \neq 0$.

Now let us take a subset of the $\mathrm{SL}_2(\mathbb{R})$ group:

$$H = \frac{1}{\sqrt{a}} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

such that $H \subset G$ and $|H| = 1$ and

$$H : x \mapsto H \cdot x = \frac{1}{\sqrt{a}} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} x = \frac{1}{\sqrt{a}} \frac{ax+b}{0x+1} = \frac{ax+b}{\sqrt{a}}$$

Now we can clearly see that the subset of the $\mathrm{SL}_2(\mathbb{R})$ group H is the affine transformation (i.e. the dilation and transformation of the real line $\mathbb{R}$) represented by $ax + b$

Now to prove that the group $ax + b$ is a subgroup, all we have to prove is that restriction of multiplication from G to H will make H a group itself, i.e. after the restrictive multiplication it will satisfy the three axioms of a group, nameley:

1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in H$.
2. Existence of Identity element.
3. Existence of an inverse for every element $g \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ where e is the identity element.

We can easily state that for any $h_1, h_2, h_3 \in H$ the property $h_1 \cdot (h_2 \cdot h_3) = (h_1 \cdot h_2) \cdot h_3$ will hold as matrix multiplication is associative. Hence this satisfies the first property of a group. Also note that the restricted multiplication of any 2 elements $h_1, h_2 \in H$ can be denoted by:

$$h_1 = \frac{1}{\sqrt{a_1}} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad h_2 = \frac{1}{\sqrt{a_2}} \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \quad \text{and}$$

$$h_1 \cdot h_2 = \frac{1}{\sqrt{a_1 a_2}} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix}$$

$$h_1 \cdot h_2 = \frac{1}{\sqrt{a_1 a_2}} \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 \\ 0 & 1 \end{pmatrix}$$

Here the composition of affine transformations is also another affine transformation and $|h_1 \cdot h_2| = 1$.

We can also see that there exists an identity element $e \in H$, where $|e| = 1$.

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

such that $h \cdot e = e \cdot h = h$ for all $h \in H$. Hence the second property of a group is also satisfied.

We can also see that there exists an inverse h^{-1} for all $h \in H$ such that:

$$h^{-1} = \sqrt{a} \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad h = \frac{1}{\sqrt{a}} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad |h^{-1}| = |h| = 1$$

So, the set H satisfies all three properties of a group and is hence a group. The set $ax + b$ of affine transformations is hence a subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Definition 12.2.3 Let X be a set and let us define, for a group G, an operation $G : X \to X$ on G on X. We say that a subset $S \subset X$ is G-Invariant if $g \cdot s \in S$ for all $g \in G$ and $s \in S$.

Question 12.2.15 Show that if $S \subset X$ is G-invariant than it's complement $X \backslash S$ is G-invariant as well.

Solution We will prove this by contradiction. Let us take an element $g \in G$ and similarly $g^{-1} \in G$. We also take $s^{'} \in X$
S such that $g \cdot s^{'} = r^{'} \in S$ and we assume that the set $X \backslash S$ is not G-Invariant, whereas the set S is G-Invariant. So, we get:

$$\begin{aligned} g \cdot s^{'} &= r^{'} \in S \\ g^{-1} \cdot g \cdot s^{'} &= g^{-1} \cdot r^{'} \\ s^{'} &= g^{-1} \cdot r^{'} \end{aligned}$$

Now, we know that S is G-Invariant for all $g \in G$ and $s \in S$. Now as $g^{-1} \in G$ and $r^{'} \in S$, $g^{-1} \cdot r^{'} \in S$. This implies that $s^{'} \in S$, but we clearly stated at the beginning that $s^{'} \in X \backslash S$ and $s^{'} \notin S$. This is clearly a contradiction. $\Rightarrow\Leftarrow$

And hence our initial assumption that $X \backslash S$ is not G-Invariant was incorrect and $X \backslash S$ is also G-Invariant. $\square$

Question 12.2.16 Find a subgroup which corresponds to the action of $ax+b$ group on $\mathbb{R}$ by the formula $(a, b) : x \mapsto ax+b$ for the point $x = 0$.

Solution

Question 12.2.17 Generate the subgroup map from the exponent map of the following zero-trace matrix

$$a(t) = exp \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}$$

Solution

$$a(t) = exp \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}$$

$$a(t) = I + \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix} + \frac{1}{2!} \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^2 + \frac{1}{3!} \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^3 + \cdots$$

We can see that for every even power of the zero-trace matrix

$$\begin{aligned} \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^2 &= \begin{pmatrix} (t/2)^2 & 0 \\ 0 & (t/2)^2 \end{pmatrix} \\ \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^4 &= \begin{pmatrix} (t/2)^4 & 0 \\ 0 & (t/2)^4 \end{pmatrix} \\ &\vdots \\ \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^{2n} &= \begin{pmatrix} (t/2)^{2n} & 0 \\ 0 & (t/2)^{2n} \end{pmatrix} \end{aligned}$$

And for the odd powers of the zero-trace matrix we have:

$$\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix} = \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}$$
$$\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^3 = \begin{pmatrix} (-t/2)^3 & 0 \\ 0 & (t/2)^3 \end{pmatrix}$$
$$\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^5 = \begin{pmatrix} (-t/2)^5 & 0 \\ 0 & (t/2)^5 \end{pmatrix}$$
$$\vdots$$
$$\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^{2n-1} = \begin{pmatrix} (-t/2)^{2n-1} & 0 \\ 0 & (t/2)^{2n-1} \end{pmatrix}$$

Using both the above results to resolve the exponential expansion, we get:

$$a(t) = exp \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}$$
$$a(t) = I + \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^2 + \frac{1}{3!}\begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix}^3 + \cdots$$
$$a(t) = I + \begin{pmatrix} -t/2 & 0 \\ 0 & t/2 \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} (-t/2)^2 & 0 \\ 0 & (t/2)^2 \end{pmatrix} + \frac{1}{3!}\begin{pmatrix} (-t/2)^3 & 0 \\ 0 & (t/2)^3 \end{pmatrix} + \frac{1}{4!}\begin{pmatrix} (-t/2)^4 & 0 \\ 0 & (t/2)^4 \end{pmatrix} + \cdots$$
$$a(t) = \begin{pmatrix} 1 + (-t/2) + \frac{(-t/2)^2}{2!} + \frac{(-t/2)^3}{3!} + \frac{(-t/2)^4}{4!} + \cdots & 0 \\ 0 & 1 + (t/2) + \frac{(t/2)^2}{2!} + \frac{(t/2)^3}{3!} + \frac{(t/2)^4}{4!} + \cdots \end{pmatrix}$$
$$a(t) = \begin{pmatrix} e^{-t/2} & 0 \\ 0 & e^{t/2} \end{pmatrix}$$

Question 12.2.18 Generate the subgroup map from the exponent map of the following zero-trace matrix:

$$a(t) = exp \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$$

Solution Expanding the exponential, we get:

$$a(t) = exp \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}$$
$$a(t) = I + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^2 + \frac{1}{3!}\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^3 + \cdots$$

Solving for all powers n of the generator matrix where $n > 2$.

$$\begin{aligned} \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^n &= \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^2 \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix}^{n-2} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & t \\ 0 & t \end{pmatrix}^{n-2} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Substituting this result in the exponential expansion we get:

$$a(t) = I + \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$a(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

Question 12.2.19 Generate the subgroup map from the exponent map of the following zero-trace matrix:

$$a(t) = exp \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}$$

Solution Expanding the exponent using the taylor-series expansion we get:

$$a(t) = I + \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} + \frac{1}{2!} + \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^2 + \frac{1}{3!} + \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^3 + \cdots$$

Solving for all even powered zero-trace matrices:

$$\begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} = \begin{pmatrix} (t/2)^2 & 0 \\ 0 & (t/2)^2 \end{pmatrix}$$
$$\begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^2 \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^2 = \begin{pmatrix} (t/2)^4 & 0 \\ 0 & (t/2)^4 \end{pmatrix}$$
$$\vdots$$
$$\begin{pmatrix} o & t/2 \\ t/2 & 0 \end{pmatrix}^{2n} = \begin{pmatrix} (t/2)^{2n} & 0 \\ 0 & (t/2)^{2n} \end{pmatrix}$$

Solving for all odd powers of the zero-trace matrix:

$$\begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^3 = \begin{pmatrix} (t/2)^2 & 0 \\ 0 & (t/2)^2 \end{pmatrix} \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} = \begin{pmatrix} (t/2)^3 & 0 \\ 0 & (t/2)^3 \end{pmatrix}$$
$$\vdots$$
$$\begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix}^{2n-1} = \begin{pmatrix} (t/2)^{2n-1} & 0 \\ 0 & (t/2)^{2n-1} \end{pmatrix}$$

Using the results of the odd and even powers of the zero-trace matrix into the exponential expansion we get:

$$a(t) = I + \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} + \frac{1}{2!} \begin{pmatrix} (t/2)^2 & 0 \\ 0 & (t/2)^2 \end{pmatrix} + \frac{1}{3!} \begin{pmatrix} 0 & (t/2)^3 \\ (t/2)^3 & 0 \end{pmatrix} + \frac{1}{4!} \begin{pmatrix} (t/2)^4 & 0 \\ 0 & (t/2)^4 \end{pmatrix} + \cdots$$
$$a(t) = \begin{pmatrix} 1 + \frac{(t/2)^2}{2!} + \frac{(t/2)^4}{4!} + \cdots & t/2 + \frac{(t/2)^3}{3!} + \frac{(t/2)^5}{5!} + \cdots \\ t/2 + \frac{(t/2)^3}{3!} + \frac{(t/2)^5}{5!} + \cdots & 1 + \frac{(t/2)^2}{2!} + \frac{(t/2)^4}{4!} + \cdots \end{pmatrix}$$
$$a(t) = \begin{pmatrix} \cosh(t/2) & \sinh(t/2) \\ \sinh(t/2) & \cosh(t/2) \end{pmatrix}$$

So, we find that:

$$\exp \begin{pmatrix} 0 & t/2 \\ t/2 & 0 \end{pmatrix} = \begin{pmatrix} \cosh(t/2) & \sinh(t/2) \\ \sinh(t/2) & \cosh(t/2) \end{pmatrix}$$

Question 12.2.20 Generate the subgroup map from the exponent map of the following zero-trace matrix:

$$a(t) = exp\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}$$

Solution Expanding the zero-trace matrix in the exponential using the Taylor-series expansion we get:

$$a(t) = exp\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}$$
$$a(t) = I + \begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^2 + \frac{1}{3!}\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^3 + \cdots$$

Solving for even powers of the zero-trace matrix, we get:

$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^2 = \begin{pmatrix} -t^2 & 0 \\ 0 & -t^2 \end{pmatrix}$$
$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^4 = \begin{pmatrix} t^4 & 0 \\ 0 & t^4 \end{pmatrix}$$
$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^6 = \begin{pmatrix} -t^6 & 0 \\ 0 & -t^6 \end{pmatrix}$$
$$\vdots$$

Solving for all odd powers of the zero-trace matrix, we get:

$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & -t^3 \\ t^3 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix}^5 = \begin{pmatrix} 0 & t^5 \\ -t^5 & 0 \end{pmatrix}$$
$$\vdots$$

Substituting the above results in the Taylor-series expansion of the zero-trace matrix we get:

$$a(t) = I + \begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix} + \frac{1}{2!}\begin{pmatrix} -t^2 & 0 \\ 0 & -t^2 \end{pmatrix} + \frac{1}{3!}\begin{pmatrix} 0 & -t^3 \\ t^3 & 0 \end{pmatrix} + \frac{1}{4!}\begin{pmatrix} t^4 & 0 \\ 0 & t^4 \end{pmatrix} + \frac{1}{5!}\begin{pmatrix} 0 & t^5 \\ -t^5 & 0 \end{pmatrix} + \cdots$$
$$a(t) = \begin{pmatrix} 1 - \frac{t^2}{2!} + \frac{t^4}{4!} + \cdots & t - \frac{t^3}{3!} + \frac{t^5}{5!} + \cdots \\ -(t - \frac{t^3}{3!} + \frac{t^5}{5!} + \cdots) & 1 - \frac{t^2}{2!} + \frac{t^4}{4!} + \cdots \end{pmatrix}$$
$$a(t) = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$$

So, we find that:

$$\exp\begin{pmatrix} 0 & t \\ -t & 0 \end{pmatrix} = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$$

12 References

The following are all the books, documents and web resources that I referred to during the period of my summer research fellowship at the Department of Mathematics, University of Auckland whilst investigating the Geometry of Möbius Transformations under Dr. Pedram Hekmati:

1. Schaum's Outlines of Complex Variables - 2nd edition
2. Lie Groups - Hollistic Overview
3. Möbius Transformations - Hollistic Overview
4. Möbius Transformations - Properties and Theorems
5. Groups and Symmetry - M. A. Armstrong [Springer - UTM]
6. Basic Topology - M. A. Armstrong [Springer - UTM]
7. Geometry of Möbius Transformations - Vladmir V. Kisil
8. Group Theory - Course Notes - J. S. Milne
9. Group Theory Introduction- Brilliant.org
10. Lagrange's Theorem
11. Geometry of Möbius Transformations - John Olsen
12. Transformation Groups - Prof. D. Joyce, Clarke Univerity
13. Permutation Group - Overview
14. Group Homomorphisms - Overview
15. Homomorphisms - Keith Conrad
16. Continous Groups - Wolfram MathWorld
17. Continuous Groups - Introductory Algebra for Physicists - Michael W. Kirson
18. Lie Groups - Overview
19. Lie Groups - The Manifold Atlas Project
20. Geometry with an Introduction to Cosmic Topology
21. Linear Fractional Transformation - Wolfram MathWorld
22. Erlangen Program - Overview