The Platonic Solids Strike Again!

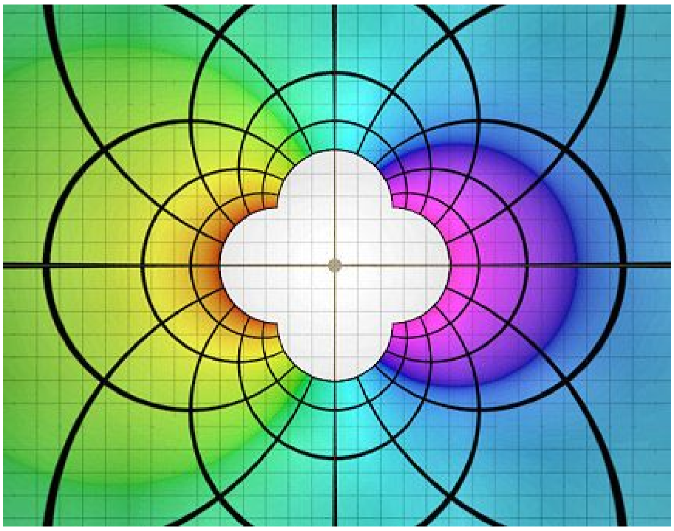
How Möbius Transformations collide with some of Mathematics' oldest characters

Fran Herr

June 2020

Abstract

In this investigation, we will examine the structure of finite groups of Möbius Transformations and how they relate to well-known symmetry groups. Most of the ideas presented are from *Complex Functions: An Algebraic and Geometric Viewpoint* by Gareth Jones and David Singerman [9]. Jones and Singerman based many of their proofs on those in *Groups of Elliptic Linear Fractional Transformations* by Ullman and Lyndon [11] as well as earlier work by Klein [10]. Along the way, we will learn about Möbius Transformations in general, some basic group theory, conjugacy classes of Möbius Transformations, and rotations of the Riemann Sphere. The journey is exciting and at times challenging, but the end result is well worth the toil.



Contents

Möbius Transformations

The Basics

A Möbius Transformation, or Linear Fractional Transformation, is a complex function of the form

$$T(z) = \frac{az+b}{cz+d} \tag{1}$$

where $a, b, c, d \in \mathbb{C}$. This may look unassuming at first, but these transformations have some extremely interesting properties. If we take the derivative of the transformation, we have

$$T'(z) = \frac{ad-bc}{(cz+d)^2}$$

If $ad - bc = 0$, then the derivative is always zero and T is constant. Constant functions do not have the properties that we are looking for and so we must require that $ad - bc \neq 0$.

Möbius Transformations describe all the automorphisms[1] of the extended complex plane. This statement can be proved with the tools we have now, but it will seem obvious as we proceed and think about Möbius Transformations from other perspectives.

Another important initial observation is that the composition of two Möbius Transformation is also a Möbius Transformation. That is, suppose we have two transformations,

$$T(z) = \frac{az+b}{cz+d} \qquad \text{and} \qquad S(z) = \frac{\alpha z+\beta}{\gamma z+\delta}$$

Then, if we consider the composition $(T \circ S)(z)$, we have

$$(T \circ S)(z) = \left(a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)+b\right)\Big/\left(c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right)+d\right) = \frac{(a\alpha+b\gamma)z+a\beta+b\delta}{(c\alpha+d\gamma)z+c\beta+d\delta}$$

This new function is also a Möbius Transformation. Thus, Möbius Transformations are "closed under composition"[2].

One way to characterize Möbius Transformations is by the number of fixed points. If T is given by (1), then a fixed point of T satisfies

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

If we manipulate this equation, then we have

$$cz^2 + (d-a)z - b = 0$$

So if z is a fixed point of T, then it is the solution to a quadratic equation. A quadratic equation has either 1 or 2 solutions, so every Möbius Transformation has 1 or 2 fixed points. If T has 3 fixed points, then it must be the identity transformation and have infinitely many fixed points.

[1] An automorphism is an isomorphism (a bijective map in the context of sets) from an object to itself

[2] This statement will be explained in the next section

Building Blocks

Consider a transformation T_0 of the form given by (1) but with $c = 0$.

$$T_0(z) = \frac{a}{d}z + \frac{b}{d}$$

Now, take another transformation T_1 in the form given by (1) but this time with $c \neq 0$.
We can rewrite T_1 in the following way,

$$T_1(z) = \frac{a}{c} - \frac{1}{c(cz + d)}$$

In these forms, we can see that all Möbius Transformations are compositions of three basic types of complex functions: translations ($f(z) = z + t,\ t \in \mathbb{C}$), scalar multiplication ($f(z) = rz,\ r \in \mathbb{C}$), and inversions ($f(z) = \frac{1}{z}$). [3]
Both translations and scalar multiplication are analytic on the entire complex plane. An inversion, on the other hand, is undefined at 0 so it is not analytic on $\mathbb{C}$. To reconcile this, we can expand the domain and codomain. The **extended complex plane** is defined to be $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. To work with the point ∞, we define the following properties:

$$\frac{1}{0} = \infty \quad \text{and} \quad \frac{1}{\infty} = 0$$

This allows the inversion to extended continuously and analytically over the whole of $\overline{\mathbb{C}}$. To see this, observe that $f'(z) = \frac{d}{dz}(z^{-1})$ is continuous at both 0 and ∞.

$$f'(0) = \lim_{z \to 0} -\frac{1}{z^2} = \infty \qquad f'(\infty) = \lim_{z \to \infty} -\frac{1}{z^2} = 0$$

Since translations and scalar multiplication are entire functions, they also extend analytically to $\overline{\mathbb{C}}$. Altogether, we can say that any Möbius Transformation is the composition of analytic functions on $\overline{\mathbb{C}}$ and so it is also analytic on $\overline{\mathbb{C}}$. Furthermore, we know that the derivative can never be zero (since we require $ad - bc \neq 0$). Thus, T is conformal[4] and it has an inverse.

Getting Spherical

The real beauty of Möbius Transformations shows itself when we think about them from the standpoint of a three-dimensional sphere. Imagine a sphere sitting embedded in the complex plane. The equator of the sphere lines up with the unit circle; the north pole, N, is at the point $(0, 0, 1)$ and the south pole, S, is at $(0, 0, -1)$. For any point on the sphere $p \neq N$, we can draw a line from N through p. Continuing the line, we eventually intersect the complex plane. This is called a **stereogaphic projection**.

[3] We will later see that the scalar multiplication case can be split up further into *rotations* and *dilations*
[4] T preserves angles and orientation between curves.

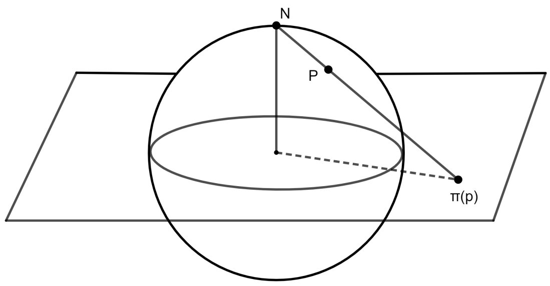


Figure 1: Stereographic Projection of p

One can think of illuminating the sphere by a single light positioned at the north pole and projecting it onto the plane. As the points on the sphere get closer to N, the corresponding projection onto $\overline{\mathbb{C}}$ moves farther from the origin. In this way, we say that N is mapped to ∞ under the projection. Since we can relate the extended complex plane to the unit sphere $\mathbb{S}^2$ in this way, we call $\overline{\mathbb{C}}$ the **Riemann Sphere** and we will denote it using Σ. The stereographic is given explicitly by

$$\pi : \mathbb{S}^2 \to \Sigma, \qquad \pi(X, Y, Z) = \frac{X + iY}{1 - Z}$$

where $p = (X, Y, Z)$ is a point on $\mathbb{S}^2 \subset \mathbb{R}^3$. This expression can be derived by parameterizing $\mathbb{S}^2$ using spherical coordinates. We will not use this formula often in our discussion, so we will leave its derivation to the reader. In addition, an explicit formula for the inverse of π can be written down. This means that π and π^{-1} must both be bijective.

Theorem 1. *The stereographic projection $\pi : \mathbb{S}^2 \longrightarrow \Sigma$ is a bijective map.*

Associating Σ with a unit sphere through stereographic projection gives a visual way to understand Möbius Transformations. Every Möbius Transformation is correlated with **rigid motions of the sphere**. These are movements of $\mathbb{S}^2$ that do not deform it in any way; they include translations and rotations. Examples of these are shown in Figure 2.

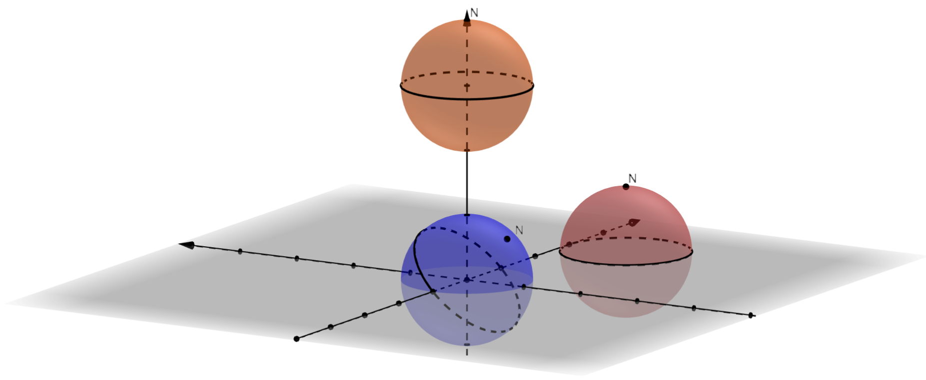


Figure 2

A translation of the sphere in the X direction and Y direction will simply translate Σ in the same way. This corresponds to a Möbius Transformation of the form $T(z) = z + t$ where $t \in \mathbb{C}$. An example of this motion is demonstrated by the red sphere in Figure 2

A translation of the sphere in the Z direction will dilate or contract the extended complex plane. This corresponds to a transformation of the form $T(z) = rz$ where $r \in (0, \infty)$. If $r < 1$, then $\mathbb{S}^2$ is moved in the negative Z direction and Σ undergoes a contraction. If $r > 1$, then $\mathbb{S}^2$ is moved in the positive Z direction and Σ undergoes a dilation. An example of a dilation is shown by the orange sphere in Figure 2.

Rotations are slightly trickier to categorize, but there are some things that we can say. If $\mathbb{S}^2$ is rotated about the Z axis, then Σ is simply rotated about the origin by the same angle. This corresponds to a transformation of the form $T(z) = e^{i\theta}z$. If $\mathbb{S}^2$ is rotated π radians around the Y axis,[5] then the points ∞ and 0 are inverted. This motion corresponds to an inversion of the form $T(z) = \frac{1}{z}$. An example of a rotation is shown by the blue sphere in Figure 2.

With this insight, we can at least gain an intuitional understanding for why Möbius Transformations are all the automorphisms of Σ. Rigid motions of $\mathbb{S}^2$ maintain the bijectivity of π. Since rigid motions are automophrisms of $\mathbb{S}^2$ they are also automorphisms of Σ. If the reader would like to see a visualization of this correlation between rigid motions of Σ and Möbius Transformations, I encourage them to watch the short video *Möbius Transformations Revealed* [4].

Matrices

It is also useful to consider Möbius Transformations from the perspective of matrices. We can associate each Möbius Transformation with a 2x2 matrix of its coefficients. If we have a transformation given by (1), then we associate it with

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

Notice that this representation is not unique. Consider the matrix αA where $\alpha \in \mathbb{C}$. This matrix gives the same transformation as A.

$$\alpha A = \begin{bmatrix} \alpha a & \alpha b \\ \alpha c & \alpha d \end{bmatrix} \qquad T(z) = \frac{\alpha az + \alpha b}{\alpha cz + \alpha d} = \frac{az + b}{cz + d}$$

This insight gives us a way to standardize all Möbius Transformations so we can characterize them by their coefficients (up to multiplication by -1).

Theorem 2. *Every Möbius transformation can be written in the form*

$$T(z) = \frac{az + b}{cz + d} \qquad \text{such that} \quad ad - bc = 1$$

Proof. Given a Möbius transformation T, suppose $ad - bc = \alpha$. We know that $\alpha \neq 0$ since Möbius Transformations are not constant. Now, define new coefficients by

$$a' = \frac{a}{\sqrt{\alpha}} \qquad b' = \frac{b}{\sqrt{\alpha}} \qquad c' = \frac{c}{\sqrt{\alpha}} \qquad d' = \frac{d}{\sqrt{\alpha}}$$

[5] or any line in Σ passing through the origin

A new transformation with these coefficients is simply another form of T.

$$\frac{a'z+b'}{c'z+d'} = \frac{\frac{1}{\sqrt{\alpha}}(az+b)}{\frac{1}{\sqrt{\alpha}}(cz+d)} = T(z)$$

These coefficients satisfy the desired property.

$$a'd'-b'c' = \frac{a}{\sqrt{\alpha}}\frac{b}{\sqrt{\alpha}} - \frac{c}{\sqrt{\alpha}}\frac{d}{\sqrt{\alpha}} = \frac{1}{\alpha}(ad-bc) = \frac{1}{\alpha}(\alpha) = 1$$

□

Remark: This representation is not unique; we could have instead multiplied all the coefficients $-\frac{1}{\sqrt{\alpha}}$. These new coefficients would also satisfy the condition that $a'd'-b'c'=1$. Moving forward, we will often choose the coefficients of T so that $ad-bc=1$. This makes calculations easier and limits the number of possible matrices that T is associated with.

Recall the observation that the composition of two Möbius Transformations is also a Möbius Transformation. This property also appears in the matrix representations of transformations. Let T and S be two transformations as given earlier. After doing calculations, we see that the product of the matrices is the matrix associated with $T \circ S$.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a\alpha+b\gamma & a\beta+d\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{bmatrix}$$

This is an extremely useful property because it allows us to compose Möbius Transformations by performing matrix multiplication instead of more complicated algebra. In addition, because matrices hold the property that the determinant of the product is the product of the determinant, if $ad-bc = \alpha\delta-\beta\gamma = 1$, then $T \circ S$ will also have determinant 1.
Moving forward, I will often equate a Möbius Transformation with a matrix. When I do this, I simply mean that the transformation and matrix are related as we have discussed.

Transformations are Transitive

We have already shown that every Möbius Transformation is conformal and so this implies that each transformation has an inverse as well. If T is the form given by (1) then T^{-1} is given by:

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

Notice that if we write T in the form such that $ad-bc=1$, then the 2x2 matrix associated with T^{-1} is the inverse of the matrix associated with T.

Theorem 3. *Given two triples of distinct elements in Σ, (z_0, z_1, z_2) and (w_0, w_1, w_2), there is a unique Möbius transformation T such that $T(z_0)=w_0$, $T(z_1)=w_1$, and $T(z_2)=w_2$.*

Proof. Since all Möbius transformations have an inverse it suffices to show that for any triple of distinct points in Σ, (z_0, z_1, z_2), there is a unique transformation U such that

$$U(z_0)=0 \qquad U(z_1)=1 \qquad U(z_2)=\infty$$

Then, we can find such a transformation, V for (w_0, w_1, w_2) as well. This would give us,

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

where T satisfies the properties stated in the problem.
We will start by showing existence of this map. First, assume that none of z_0, z_1, z_2 is ∞. Then, let U be given by

$$U(z) = \frac{(z - z_0)(z_1 - z_2)}{(z - z_2)(z_1 - z_0)} = \frac{(z_1 - z_2)z - z_0(z_1 - z_2)}{(z_1 - z_0)z - z_2(z_1 - z_0)}$$

U is a Möbius Transformation since we can write it in the standard form. And we see that

$$U(z_0) = \frac{(z_0 - z_0)(z_1 - z_2)}{(z_0 - z_2)(z_1 - z_0)} = 0 \qquad U(z_1) = \frac{(z_1 - z_0)(z_1 - z_2)}{(z_1 - z_2)(z_1 - z_0)} = 1 \qquad U(z_2) = \lim_{z \to z_2} \frac{(z - z_0)(z_1 - z_2)}{(z - z_2)(z_1 - z_0)} = \infty$$

So U has the desired property. Now, if any of the z_j's is ∞ we simply define U to be the limit of this transformation as that point approaches ∞. For example, suppose that $z_1 = \infty$. Then, we define U to be

$$U(z) = \lim_{z_1 \to \infty} \left[\frac{(z - z_0)(z_1 - z_2)}{(z - z_2)(z_1 - z_0)} \right]$$

$$= \lim_{z_1 \to \infty} \left[\frac{(z - z_0)(1 - \frac{z_2}{z_1})}{(z - z_2)(1 - \frac{z_0}{z_1})} \right]$$
$$= \frac{z - z_0}{z - z_2}$$

We can find a similar U if either of the other points is ∞.

Now, we will show uniqueness of U. Suppose that there are two transformations, U_1 and U_2 that map the triple (z_0, z_1, z_2) to $(0, 1, \infty)$. Then both U_1^{-1} and U_2^{-1} must map $(0, 1, \infty)$ to (z_0, z_1, z_2). Thus, the composition $U_1^{-1} \circ U_2$ fixes three points– z_0, z_1, and z_2– and it must be the identity. This means that U_1^{-1} is the inverse of U_2 and so $U_1 = U_2$. Therefore, the map U that sends (z_0, z_1, z_2) to $(0, 1, \infty)$ is unique. □

Intuitional Pitfalls

Before we move on with the discussion, I wanted to address some "intuitional pitfalls" that have arisen for myself. My confusion came down to this: when we perform stereographic projection *from the unit sphere to the extended complex plane*, we project from the north pole of the sphere *as it is positioned in space*. If we have translated the sphere so that N is no longer on the Z axis, then we still project from that point. However, when perform the inverse of stereographic projection, *from the extended complex plane to the unit sphere*, we always map Σ onto $\mathbb{S}^2$ with the north pole positioned at $(0, 0, 1)$.

This means that if we start with the sphere, translate it far away from the origin, project it onto the complex plane, and then invert that projection, it can appear that we have distorted the surface of the sphere. A pair of points that was once antipodal[6] can now appear rather close together. This is

[6] Antipodal points are on opposite sides of the sphere. A line defined by two antipodal points will pass through the center of the sphere.

counter-intuitive because under rigid motions, the sphere itself is never deformed. The deformation comes from the change in perspective because of translation. In this way, movements consisting of pure rotations are the only ones we can be sure to preserve antipodal points. Even though, relative to the placement of the sphere, translations preserve antipodal points as well.

This can be seen in Figure 3. The red sphere is a translated version of $\mathbb{S}^2$. The points X and X' are antipodal on the red sphere. But after performing π followed by π^{-1}, the image points Y and Y' are no longer antipodal.

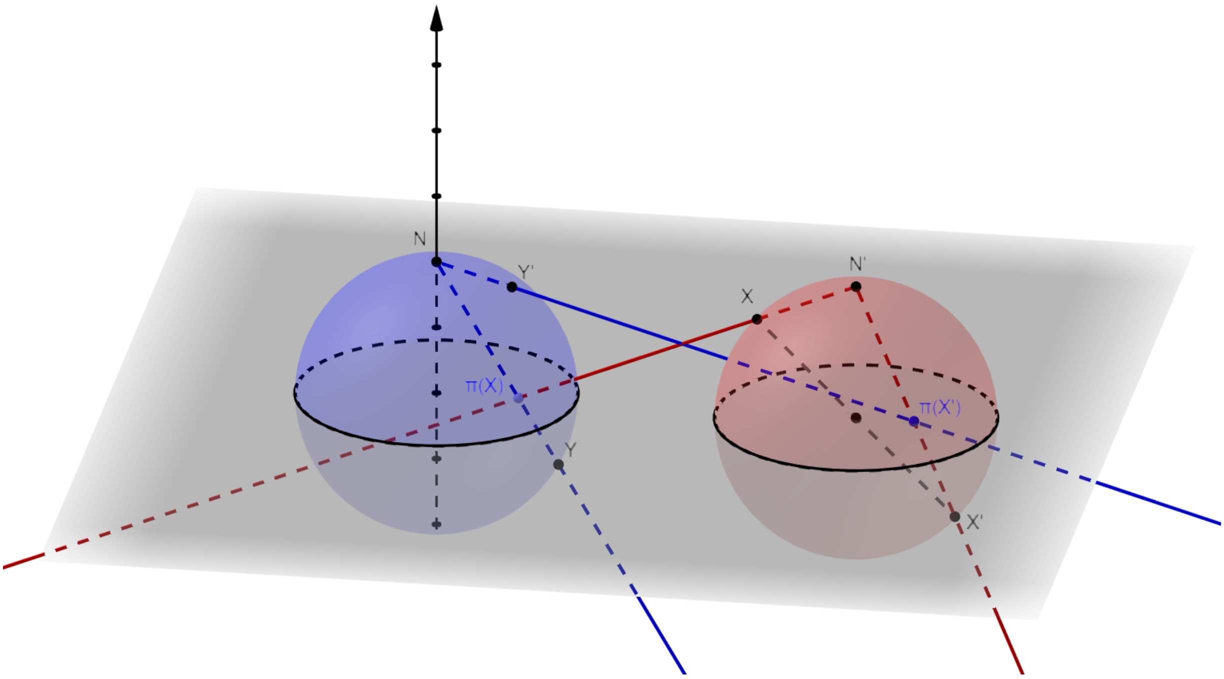


Figure 3

Basic Group Theory

Some Definitions

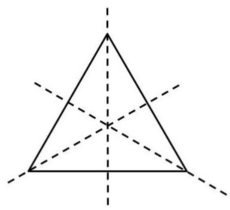
Definition 1. *A **Group** consists of an underlying set G and an operation $(\cdot)$. Sometimes we will denote the group as $(G, \cdot)$ but often we will simply use G when the operation is implied. The Group and its operation must satisfy the following properties:*

- *There is an identity element $e \in G$ such that for every $g \in G$, $e \cdot g = g \cdot e = g$.*
- *For each $g \in G$, there is some $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$*
- *The operation is associative. If $g, h, k \in G$, then $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.*

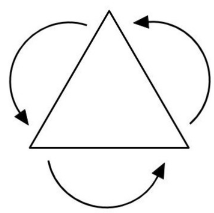
Notice that the operation does not have to be commutative. It may be true that $g \cdot h \neq h \cdot g$. Most elementary operations are commutative and so this can be counter-intuitive to readers who are new to group theory.

The integers and the addition operation, $(\mathbb{Z}, +)$, are an example of a group. The identity element is 0 since for any $n \in \mathbb{Z}$, $0 + n = n$. The inverse of each element is its opposite since $n + -n = 0$. The sum of two integers is always an integer, and addition is associative.

Another example is the symmetry group of a regular polygon with n sides. We call this a **dihedral group** and denote it D_{2n}. For instance, consider all the symmetries of an equilateral triangle. There are three symmetrical reflections– one for each side– and three rotations– 120°, 240°, and 360°. The group operation is simply "adding" the actions by performing one and then another. Any combination of these actions will be a symmetry action on the triangle. Each reflection is its own inverse and each rotation of n degrees has an inverse rotation of $360 - n$ degrees.



Reflections of the Triangle



A Rotation

Also, notice that a group can either be **infinite** or **finite**. The integers are an infinite group and D_{2n} is a finite group. This distiction depends on whether the underlying set has infinitely many or finitely many elements. The **order of** G, $|G|$ is the number of elements in G. If G is infinite, then $|G| = \infty$. The **order of an element** $g \in G$ is the smallest integer m such that $g \cdot g \cdots g = g^m = e$. If G is infinite, then there is at least one element that does not have a finite order. If G is finite, then every element has a finite order.

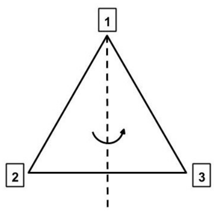
Definition 2. *Let $(G, \cdot)$ and $(H, *)$ be two groups. A **group homomorphism** $\varphi : G \to H$ is a set function from G to H. If $g_1, g_2 \in G$, φ must satisfy the property that*

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) * \varphi(g_2)$$

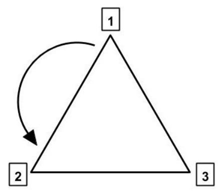
Definition 3. *A* ***group isomorphism*** *is a homomorphism φ that is a bijection between G and H. Equivalently, a group homomorphism is an* ***isomorphism*** *if it has an inverse.*

Definition 4. *Two groups G and H are* ***isomorphic*** *if there a group isomorphism from G to H.*

Another example of a group is the permutations of the set $\{1, 2, 3\}$, denoted S_3. This group has order $3! = 6$. We will denote an element of S_3 as an ordered triple of 1, 2, and 3 (e.g $(3, 1, 2) \in S_3$). We can find a group isomorphism between D_6 and S_3. Each vertex of the triangle is associated with an element in $\{1, 2, 3\}$ and every permutation of the vertices can be obtained by a symmetry action. Some examples of this correlation are shown below:



Corresponds to $(1, 3, 2)$



Corresponds to $(3, 1, 2)$

Definition 5. *Let $(G, \cdot)$ be a group and let H be a subset of G. H is a* ***subgroup*** *of G ($H \leq G$) if it satisfies the following properties:*

- *H contains the identity element of G ($e \in H$).*
- *If $h \in H$, then $h^{-1} \in H$*
- *If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$*

Remark: These conditions can all be encompassed by a single requirement: if $a, b \in H$, then $a \cdot b^{-1} \in H$. However, I believe it is more helpful to see the three stated results of this one condition. This reveals that a subgroup of G is simply a smaller group contained inside of G.

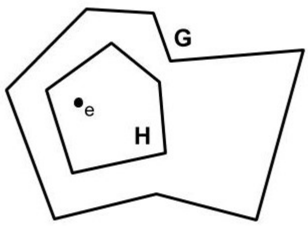


Figure 4: H as a subgroup of G

Every group has at least two subgroups, the trivial group, $\{e\}$ and the group itself. One can check that both of these are indeed subgroups of G. A nontrivial subgroup of $(\mathbb{Z}, +)$ is all the even integers, $(2\mathbb{Z}, +)$. For any two even integers, n and m, $n - m$ is even. So the even integers satisfy the single condition for a subgroup. One subgroup of D_{2n} is the set of only rotation elements. The rotation of 360° is the identity element, the inverse of a rotation is also a rotation, and the composition of two rotations is still a rotation.

Lagrange's Theorem

Definition 6. *Let G be a group and H be a subgroup of G. If $g \in G$, the* ***coset*** *of H given by g is $gH = \{g \cdot h : h \in H\}$.*

Definition 7. *The* ***index*** *of H in G, denoted $[G : H]$, is the number of distinct cosets of H. That is, it is the size of $\{gH : g \in G\}$.*

Remark: Note that the cosets are *not necessarily subgroups themselves.* If $g \in H$, then $gH = H$ and so in this case, gH is a subgroup. However, if $g \notin H$, then $g^{-1} \notin H$ and so there is no $h \in H$ such that $g \cdot h = e$. This means that gH does not contain the identity element and thus cannot be a subgroup.

This brings us to one of the most important theorems in group theory. The proof given for this result is modeled after that in [7].

Theorem 4 (Lagrange's Theorem)**.** *Let G be a finite group, H be a subgroup of G, and $[G : H]$ be the index of H in G. Then $|G| = |H| \cdot [G : H]$.*

Proof. Let $|G| = N$. First, notice that Lagrange's Theorem holds for both the trivial subgroup and the group G itself.

$$|\{e\}| = 1 \quad \text{and} \quad [G : \{e\}] = |\{g \cdot e : g \in G\}| = N$$

And we have $N = 1 \cdot N$. Similarly for G,

$$|G| = N \quad \text{and} \quad [G : G] = |\{gG : g \in G\}| = 1$$

And so $N = N \cdot 1$. Now that we have established that the theorem is true in the trivial cases, let $H < G$ be a proper subgroup of G such that $H \neq \{e\}$. The index of H in G is the number of distinct cosets. In order to prove Lagrange's Theorem, we will show that none of these cosets overlap and that each is the same size as H. Then, since every element of G is in a coset of H, this will prove the desired result. First, we will show that no two cosets overlap.
Suppose that there is is a coset g_1H and chose $g_2 \notin g_1H$. For contradiction, suppose g_1H and g_2H overlap. Then there are some $h_i, h_j \in H$ such that $h_i, h_j \neq e$ and

$$g_1 \cdot h_i = g_2 \cdot h_j$$

But then we would have

$$g_1 \cdot h_i \cdot h_j^{-1} = g_2$$

Since H is a subgroup, we can be sure that $h_i \cdot h_j^{-1} \in H$ and so we must have $g_2 \in g_1H$ which is a contradiction. Hence, we do not have any overlap between distinct cosets. Note that this also shows that if $g_2 \notin H$, then g_2H does not overlap with H at all. One can simply choose $g_1 \in H$ and the argument follows the same way.
Now for the uniform size of cosets. If we know that coset multiplication is one-to-one, then we would

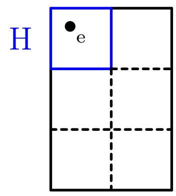
certainly have $|gH| = |H|$ for all $g \in G$ since we would have a bijective map between finite sets[7]. For contradiction, suppose that coset multiplication is not one-to-one and there are some $h_1, h_2 \in H$ such that $g \cdot h_1 = g \cdot h_2$. Then, we have

$$g \cdot h_1 = g \cdot h_2 \quad \Rightarrow \quad g^{-1} \cdot g \cdot h_1 = h_2 \quad \Rightarrow \quad h_1 = h_2$$

Hence, these cannot be distinct elements of H and coset multiplication must be one-to-one. So, we have $m = [G : H]$ distinct cosets of H in G, none of them overlap, each has size $|H|$, and their union contains all of G. Then, it must be true that

$$|G| = |H| \cdot [G : H]$$

□



G divided into cosets by H

Lagrange's Theorem gives us a way to relate the size of a group and to the size of any subgroups it may have. It tells us that the size of a subgroup must always divide the size of the group. Beyond that, we can apply this result to subsequent ideas in group theory in order to develop tools to uncover the structure of a group.

Conjugation

Conjugation of an element and a group allows us to perform a "change of basis" in a general sense. We can move to a space, perform a certain action, and then return from that space.

Definition 8. *Suppose that G is a group and $g_1, g_2 \in G$. These elements are **conjugate** in G if there is some $h \in G$ such that $g_1 = h \cdot g_2 \cdot h^{-1}$.*

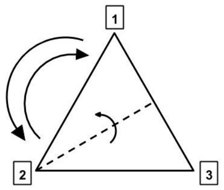
Notice that conjugation is bidirectional. If $g_1 = h \cdot g_2 \cdot h^{-1}$, then $g_2 = h^{-1} \cdot g_1 \cdot h$. Conjugation is also transitive. Suppose that $g_1, g_2, g_3 \in G$, g_1 is conjugate to g_2, and g_1 is conjugate to g_3. Then g_2 is conjugate to g_3. To see this, let $g_1 = h_2 \cdot g_2 \cdot h_2^{-1}$ and $g_1 = h_3 \cdot g_3 \cdot h_3^{-1}$. Then we have

$$h_2 \cdot g_2 \cdot h_2^{-1} = h_3 \cdot g_3 \cdot h_3^{-1} \quad \Longrightarrow \quad g_2 = h_2^{-1} h_3 \cdot g_3 \cdot h_3^{-1} h_2$$

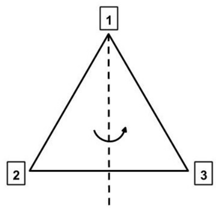
And so g_2 is conjugate to g_3 by $h_2^{-1} \cdot h_3$. With this insight, we can split a group G into its **conjugacy classes**. These are disjoint subsets of G, $(C_1, C_2, \ldots C_n)$ such that if $g_1, g_2 \in C_i$, then g_1 and g_2 are conjugate in G.

[7]The surjectivity of coset multiplication is implicit in the definition.

Conjugate elements often have similar properties. For instance, consider the elements of D_6 corresponding to $r_1 = (1,3,2)$ and $r_2 = (3,2,1)$. These are both reflections– r_1 reflects across the symmetry line through vertex 1 and r_2 does so across the line through vertex 2. If we rotate the triangle so vertex 1 meets vertex 2, perform r_2, and then rotate the triangle back, we have the same result as simply performing r_1. Hence, these reflections are conjugate under a rotation.



[rotation]$^{-1}r_2$[rotation]



r_1

Notice that these two symmetry actions have the same number of fixed points– namely, one. In fact, any element of S_3 which corresponds to a reflection in D_6 has 1 fixed point. An element of S_3 that corresponds to a rotation has no fixed points. All of the reflections in S_3 form one conjugacy class, and all of the rotations form another. So the conjugacy classes can be characterized by their fixed points. We will come back to this idea in the next section.

Group Actions

Now, we encounter the primary use of groups: as actions on a set of objects. We have already seen an example of this; the symmetry group D_{2n} *acts on* a regular polygon with n sides.

If G is a group that acts on a set A, then every $g \in G$ determines a unique isomorphism of A. That is, for every $g \in G$, there is some $\varphi_g : A \to A$ determined by g which is a bijection. Each element of G contains unique instructions for how to map A onto itself. Often, we will simply denote an action of $g \in G$ on $a \in A$ as $g(a)$. Group actions must also satisfy the following condition. If $g, h \in G$, then

$$(g \cdot h)(a) = g(h(a))$$

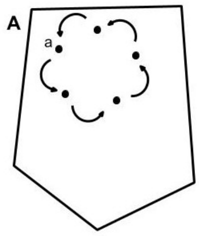
Notice that this is analogous to the requirement that group operations must be associative. In fact, this property exists *exactly because* group operations are associative. Associating each g with a map φ_g can be framed as a group homomorphism between the elements of G and the set of automorphisms of A. There are two sets that arise from group actions that we would like to discuss here.

Definition 9. *The **stabilizer** of an element $a \in A$ is the set of $g \in G$ such that $g(a) = a$.*

$$Stab(a) = \{g \in G : g(a) = a\}$$

Definition 10. *An element $b \in A$ is in the **orbit** of $a \in A$ if there is some $g \in G$ such that $g(a) = b$.*

$$Orbit(a) = \Omega_a = \{b \in A : \exists g \in G,\ g(a) = b\}$$



The orbit of $a \in A$

Notice that the *stabilizer* is a subset of the *group* G and the *orbit* is a subset of the *set* A. These two sets exist in different spaces, but they are related as we shall see shortly. Another interesting observation is that for every $a \in A$, $\mathrm{Stab}(a)$ is a subgroup of G. Suppose that $g, h \in \mathrm{Stab}(a)$ then, it must be true that $g \cdot h^{-1}$ is in $\mathrm{Stab}(a)$ as well.

$$(g \cdot h^{-1})(a) = g(h^{-1}(a)) = g(a) = a$$

And so $\mathrm{Stab}(a)$ satisfies the condition for subgroups.
Thus, we can apply Lagrange's Theorem to the stabilizer.

$$|G| = |\mathrm{Stab}(a)| \cdot [G : \mathrm{Stab}(a)]$$

With this information, we can reveal the relationship between the stabilizer and the orbit.

Theorem 5 (Orbit-Stabilizer Theorem)**.** *Let G be a finite group that acts on a set A and let Ω_a be the orbit of an element $a \in A$. Then for every a,*

$$|\Omega_a| = [G : Stab(a)]$$

Proof. Every element of G either moves a to an element of its orbit or keeps a the same. We know that the index $[G : \mathrm{Stab}(a)]$ is the number of distinct cosets of $\mathrm{Stab}(a)$ in G. So, if we show that two actions which send a to the same element of Ω_a determine the same coset of $\mathrm{Stab}(a)$, then we know that $[G : \mathrm{Stab}(a)]$ is given by the number of elements in the orbit of a.
Suppose that $g_1, g_2 \in G$ and that $g_1(a) = g_2(a)$. Then, by properties of group actions, we also have

$$(g_2^{-1} \cdot g_1)(a) = a$$

This tells us that $g_2^{-1} \cdot g_1 = t$ for some $t \in \mathrm{Stab}(a)$ and consequently $g_1 = g_2 \cdot t$. Now, consider the cosets of $\mathrm{Stab}(a)$ given by g_1 and g_2.

$$g_1\mathrm{Stab}(a) = g_2(t\mathrm{Stab}(a)) = g_2\mathrm{Stab}(a)$$

Thus, both elements determine the same coset of $\mathrm{Stab}(a)$ and we have $[G : \mathrm{Stab}(a)] = |\Omega_a|$. $\square$

The Orbit-Stabilizer Theorem along with application of Lagrange's Theorem to the stabilizer group allows us to make the following very useful assertion.

Corollary 1. *If G is a finite group that acts on a set A and $a \in A$, then*

$$|G| = |\Omega_a| \cdot |Stab(a)|$$

This result tells us that all elements in the same orbit have the same size stabilizer. With this result in hand, we can prove another important theorem for group actions.

Theorem 6 (Burnside's Lemma)**.** *Let G be a finite group that acts on a set A. Let $|A^g|$ be the number of elements in A that are fixed by $g \in G$ ($A^g = \{a \in A : g(a) = a\}$). Then,*

$$|A/G| = \frac{1}{|G|} \sum_{g \in G} |A^g|$$

where $|A/G|$ denotes the number of orbits in A.

Proof. To start, we can express the sum $\sum_{g \in G} |A^g|$ as the size of the following set:

$$\{(a, g) : a \in A, g \in G,\ g(a) = a\}$$

Currently, the sum counts over all the g's in this set, but to reframe it, we can count over all the a's instead. If we fix $a_0 \in A$, then see that $\{(a_0, g) : g(a_0) = a_0\} = \text{Stab}(a_0)$. So we can rewrite the sum using the stabilizer of each $a \in A$.

$$\frac{1}{|G|} \sum_{g \in G} |A^g| = \frac{1}{|G|} \sum_{a \in A} |\text{Stab}(a)| = \sum_{a \in A} \frac{|\text{Stab}(a)|}{|G|}$$

In Corollary 1, we have shown that $|G| = |\text{Stab}(a)| \cdot |\Omega_a|$. This gives us,

$$\frac{1}{|\Omega_a|} = \frac{|\text{Stab}(a)|}{|G|}$$

This is true for each $a \in A$, and so we have,

$$\sum_{a \in A} \frac{|\text{Stab}(a)|}{|G|} = \sum_{a \in A} \frac{1}{|\Omega_a|}$$

Now, each orbit in A is disjoint and so we can break up this sum further into one over each distinct orbit. Let n denote the number of orbits in A.

$$\sum_{a \in A} \frac{1}{|\Omega_a|} = \sum_{i=1}^{n} \sum_{a \in \Omega_i} \frac{1}{|\Omega_i|}$$

Each orbit has $|\Omega_i|$ elements and so for each i, the inner sum will be 1. This gives us the desired result.

$$\sum_{i=1}^{n} \sum_{a \in \Omega_i} \frac{1}{|\Omega_i|} = \sum_{i=1}^{n} 1 = n = |A/G|$$

$\square$

Now, let us turn our attention back to the idea of conjugation. When we apply conjugation to an entire group, we have a way to formalize a "change of basis". For instance, suppose we have a group G that acts on a set A and another group H that acts on a set X. Suppose also that we have a set bijection f between A and X.

$$f : A \longrightarrow X$$

Then, we would like to be able to define a group homorphism φ between G and H that satisfies the following property. If $g \in G$ and $a \in A$, then

$$g(a) = (f^{-1} \circ \varphi(g) \circ f)(a)$$

We will explore this idea in a specific context shortly.

The Möbius Group

Finally, we come to our purpose for discussing Group Theory. The set of all Möbius Transformations form a group under composition which acts on the set Σ. We call this group $\mathsf{Möb}$. The identity transformation, $I(z) = z$, serves as the identity element of $\mathsf{Möb}$. In the previous section, we have already shown that every Möbius Transformation has an inverse which is also in $\mathsf{Möb}$, and that the composition of two Möbius Transformations is also a Möbius Transformation. And so $\mathsf{Möb}$ satisfies the properties of a group.

In addition, we have already seen two group homomorphisms involving $\mathsf{Möb}$. The group of rigid motions of $\mathbb{S}^2$ is isomorphic to $\mathsf{Möb}$. The underlying sets– Σ and $\mathbb{S}^2$– are related under stereographic projection.

We can also define a group homomorphism from $\mathsf{Möb}$ to the group of 2x2 matrices of complex numbers with determinant 1, $PSL(2, \mathbb{C})$. These groups are not isomorphic because every $T \in \mathsf{Möb}$ corresponds to two elements of $PSL(2, \mathbb{C})$.
Conceptualizing Möbius Transformations as part of a group will allow us to uncover some of their interesting properties.

Classifying Möbius Transformations

Conjugacy Classes

As we have seen in the previous section, conjugate elements have similar properties. Defining the conjugacy classes of Möb can help us understand the group structure. Recall the observation that conjugate elements in D_6 have the same number of fixed points. This is also true of Möbius Transformations. Suppose we have conjugate transformations T and S so that, for some $U \in$ Möb , $T = U \circ S \circ U^{-1}$ and let z_0 be a fixed point of S. Let $U(z_0) = w_0$. Then we observe that

$$T(w_0) = (U \circ S \circ U^{-1})(w_0) = (U \circ S)(z_0) = U(z_0) = w_0$$

So w_0 is a fixed point of T. This gives a one-to-one correspondence between the fixed points of S and those of T. With this in mind, the fixed points of a transformation can help us define its conjugacy class.

Theorem 7. *Every non-identity Möbius transformation is conjugate to some U_λ, defined as follows, for some $\lambda \neq 0$.*

$$U_\lambda(z) = \begin{cases} z + \lambda & \lambda = 1 \\ \lambda z & \lambda \neq 1 \end{cases}$$

Proof. As we have already seen, every non-identity transformation has either 1 or 2 fixed points. First, suppose that T has one fixed point, z_0. Then, by transitivity, we can find a transformation V such that $V(z_0) = \infty$. We can conjugate T by V to create a transformation with ∞ as its only fixed point.

$$(V \circ T \circ V^{-1})(\infty) = (V \circ T)(z_0) = V(z_0) = \infty$$

And so the conjugate transformation must be of the form $V \circ T \circ V^{-1}(z) = z + t$ for some $t \in \mathbb{C} \backslash \{0\}$. Now, take the transformation $W(z) = \frac{1}{t} z$ and conjugate again, this time by W.

$$(W \circ V \circ T \circ V^{-1} \circ W^{-1})(z) = z + 1 = U_1$$

Hence, if T has one fixed point, then it is conjugate to U_1 by $W \circ V$.
Now suppose that T has two fixed points, z_0 and z_1. Then, again by transitivity, we can find a transformation V such that $V(z_0) = 0$ and $V(z_1) = \infty$. When we conjugate T by V, the resulting transformation fixes both 0 and ∞.

$$(V \circ T \circ V^{-1})(0) = (V \circ T)(z_0) = V(z_0) = 0 \qquad (V \circ T \circ V^{-1})(\infty) = (V \circ T)(z_1) = V(z_1) = \infty$$

So this transformation must be of the form

$$(V \circ T \circ V^{-1})(z) = \lambda z = U_\lambda$$

for some $\lambda \in \mathbb{C} \backslash \{0, 1\}$. □

The number of fixed points gives some characterization of a Möbius Transformation, but two transformations can have the same number of fixed points and behave very differently. For instance consider the transformations

$$R(z) = e^{i\frac{\pi}{4}} z \quad \text{and} \quad D(z) = 2z$$

These both have two fixed points (in fact, they are the same two fixed points, 0 and ∞) but they look very different. This is shown in Figure 5. R is a rotation of Σ counter-clockwise by $\frac{\pi}{4}$ and D is a dilation of Σ by a factor of 2.

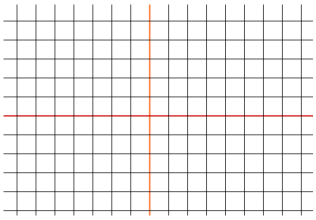
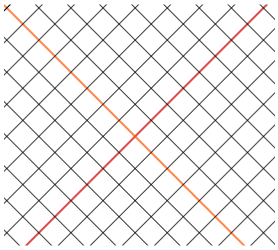
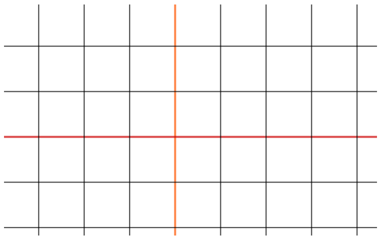


Figure 5: Σ before Transformation



$R(\Sigma)$



$D(\Sigma)$

So can we define another property of a transformation that will give us insight into how it behaves? Of course, I ask this question because the answer is yes.

Trace

The **trace** is a commonly studied property of matrices. It is simply the sum of all the diagonal entries in the matrix. For a 2x2 matrix defined by

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

we have $tr(A) = a + d$. If we wish to use this property to study Möbius Transformations, we have a problem: a given transformation is not associated with a unique matrix. This means that we could have multiple traces for the same transformation. As a first step in solving this problem, we can require that T is in the form with $ad - bc = 1$. This condition gives only two matrices that represent T.

$$+A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad -A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

To give uniqueness for the trace of a Möbius Transformation, we define the function $\tau : \mathsf{Möb} \to \mathbb{C}$

$$\tau(T) = tr^2(A)$$

where A is an associated matrix for T with determinant 1. Then, we have

$$\tau(T) = tr^2(A) = tr^2(-A) = (a + d)^2$$

and so τ gives only one value for each transformation. An important property of τ is that it remains the same after commuting transformations. That is, if T and S are two transformations, then even if $T \circ S \neq S \circ T$, it is always true that $\tau(TS) = \tau(ST)$. This can be verified by direct calculation. As a consequence of this property, conjugate elements have the same value for τ. Suppose that T and S are conjugate elements and $T = U \circ S \circ U^{-1}$. Then, because τ commutes, we have

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

So we see that conjugation preserves the trace of a transformation.

Connecting λ and τ

Now, suppose that T has one fixed point and is conjugate to U_1. Then $\tau(T) = \tau(U_1)$. In matrix form, we can write U_1 as

$$U_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Then we have $\tau(U_1) = 2^2 = 4 = \tau(T)$.
If T has two fixed points, then it is conjugate to some U_λ for $\lambda \notin \{1, 0\}$. U_λ is represented by a matrix of the form:

$$U_\lambda = \begin{bmatrix} \sqrt{\lambda} & 0 \\ 0 & \sqrt{\lambda}^{-1} \end{bmatrix}$$

This gives us

$$\tau(T) = \tau(U_\lambda) = \left(\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}}\right)^2 = \lambda + \frac{1}{\lambda} + 2$$

With this, we see that τ is a stronger characterization of transformations than the number of fixed points. It depends not only on the number of fixed points, but the conjugacy class as well.

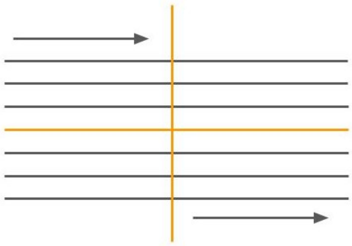
Geometric Categories of Transformations

We can use τ to separate the conjugacy classes into four main types of Möbius transformations. We will discuss each of these briefly, but only the elliptic transformations will be important for the rest of this investigation.

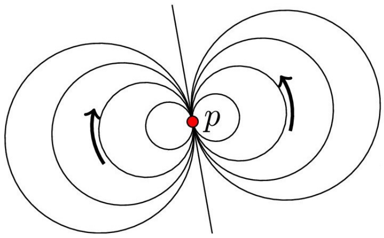
Parabolic Transformations

- One fixed point
- Conjugate to U_1
- $\tau(T) = 4$

To visualize this type of transformation, we can think about how U_1 transforms Σ. If we compose U_1 with itself many times, every point on the plane moves along a horizontal line in the positive direction. Horizontal lines in Σ correspond to circles through the north pole on $\mathbb{S}^2$. In this way, under U_1, all points on the plane move in circles that pass through ∞. For any transformation T that is conjugate to U_1, the extended complex plane is transformed in a similar way. If p is the fixed point of T, then every other point in Σ moves in a circle that passes through p. This behavior is shown in the figure below.



Fixed point ∞

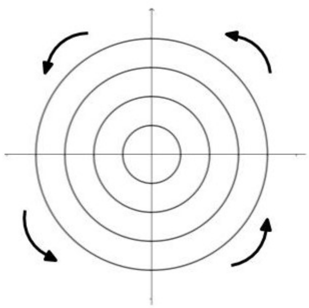


Fixed point p

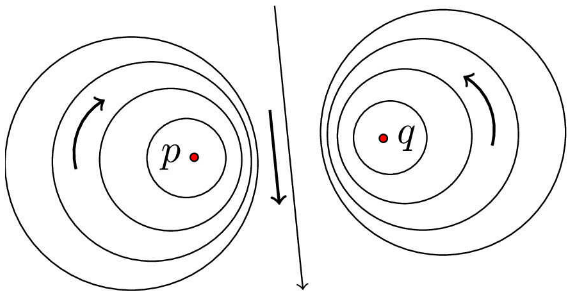
Elliptic Transformations

- Two fixed points
- Conjugate to U where $\lambda \neq 1$ and $|\lambda| = 1$
- $\tau(U_\lambda) \in \mathbb{R}$ and $0 \leq \tau(U_\lambda) < 4$

Elliptic transformations are conjugate to rotations about the origin. Upon repetition, a U_λ of this form will move all points but 0 and ∞ in circles centered at the origin. Relative to these circles, 0 and ∞ are *symmetric*. Applying this same behavior to a generalized elliptic transformation with fixed points p and q, we conclude that all other points move in symmetric circles around the two fixed points.



Fixed points 0 and ∞

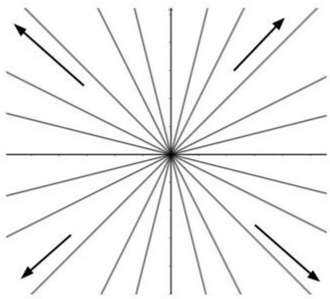


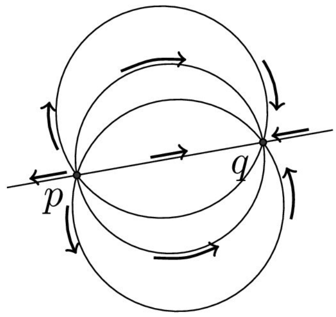
Fixed points p and q

Hyperbolic Transformations

- Two fixed points
- Conjugate to U_λ where $\lambda \in \mathbb{R}$, $|\lambda| \neq 1$
- $\tau(T) \in \mathbb{R}$ and $4 < \tau(T)$

Hyperbolic transformations are conjugate to pure dilations or contractions of Σ. This corresponds to translations of $\mathbb{S}^2$ along the Z axis. With repetition, points will move away from one fixed point and towards another. This is shown in how dilations move all nonzero points towards ∞ and contractions move all points but ∞ towards 0.


Fixed points 0 and ∞

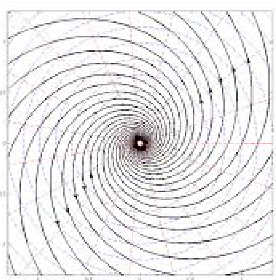


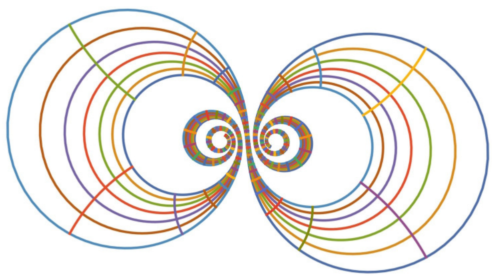
Fixed points p and q

Loxodromic Translations

- Two fixed points
- Conjugate to U_λ where $|\lambda| \neq 1$ and $\lambda \notin \mathbb{R}$
- $\tau(T) \notin \mathbb{R}$ or $\tau(T) < 0$

Loxodromic Transformations are the most complicated. They are some combination of Elliptic and Hyperbolic transformations. In the simple case, we can think of spinning $\mathbb{S}^2$ like a top as we move it along the Z axis. This moves all points but 0 and ∞ in spirals emanating from the origin. Applying this to Loxodromic Transformations in general, we conclude that non-fixed points move in spirals away from one fixed point and towards another.


Fixed points 0 and ∞


Fixed points p and q

Period of a Transformation

We have already alluded to the behavior of a transformation as we continue to let it act on Σ repeatedly. Let us investigate this idea more fully.

Definition 11. *The* ***period*** *of a Möbius Transformation T is the smallest integer n such that T composed with itself n times is the identity (i.e. $T^n = I$). If there is no such n, then we say T has an infinite period.*

Remark: Observe that this definition is equivalent to the order of T in Möb as we discussed in the group theory section.

Lemma 1. *Conjugate transformations have the same period.*

Proof. Suppose that T and S are conjugate such that $T = USU^{-1}$. First, suppose that T has a finite period, n. Then we have,

$$\begin{aligned} T^n &= (USU^{-1})^n \\ &= USU^{-1}USU^{-1} \circ \circ \circ USU^{-1} \\ &= US^nU^{-1} \end{aligned}$$

And so since $T^n = I$, then it must also be true that $S^n = I$. This tells us that the period of S is at most n. By applying the argument in the other direction, we can conclude that the period of T and of S must be the same.
Now, suppose that T does not have a finite period. For contradiction, assume that there is some m such that $S^m = I$.

$$T^m = US^mU^{-1} = UU^{-1} = I$$

This would imply that T has a finite period, a contradiction. Hence, if T has an infinite period, then S does as well. $\square$

If G is a finite group, then every element of G must have a finite order. So in order to characterize the finite subgroups of Möb , we need to know which Möbius Transformations have a finite period. Well, because of Lemma 1, we can simply determine which U_λ can have a finite period. If U_λ has a finite period, then all members of its conjugacy class do as well.

Theorem 8. *If T is a non-identity Möbius transformation with a finite period, then T is elliptic.*

Proof. First, let's take a look at $U_1 = z + 1$. For any integer $m > 0$, we see that $U_1^m(z) = z + m$. So because the period of a transformation must be strictly greater than zero, U_1 cannot have a finite period. Thus, by Lemma 1, no Parabolic transformations have a finite period.

Now, consider U_λ for $\lambda \notin \{1, 0\}$. For any integer $m > 0$, we have $U_\lambda^m(z) = \lambda^m z$. In order for there to be some m such that $U_\lambda^m = I$, we must have $\lambda^m = 1$. This means that λ must be an m^{th} root of unity and $|\lambda| = 1$. Thus, if U_λ has a finite period then it must be elliptic. So, again because of Lemma 1, only elliptic transformations can have finite periods. $\square$

Remark: Note that this theorem only goes in one direction. It is not true that all elliptic transformations have a finite period. If $|\lambda| = 1$ but λ is not a root of unity for any integer m, then U_λ will be elliptic but it will not have a finite period.

Rotations of the Riemann Sphere

Defining Rotations of Σ

Definition 12. *A Möbius Transformation T is a* ***rotation of Σ*** *if it is conjugate to a rotation of $\mathbb{S}^2$ under stereographic projection. That is, for some rotation of the sphere Φ, we have*

$$T = \pi \circ \Phi \circ \pi^{-1}$$

We denote the group of rotations as $\mathrm{Rot}(\Sigma)$. Notice that $\mathrm{Rot}(\Sigma)$ is a subgroup of Möb . We consider the identity transformation to be a rotation of angle zero[8]. Suppose that T is conjugate to a rotation of $\mathbb{S}^2$ around an axis though points p and $-p$ of an angle ϕ. Then T^{-1} is conjugate a rotation of $-\phi$ around the same axis. So if T is a rotation, then T^{-1} surely is as well. Finally, the composition of two rotations is also a rotation.

We would like to be able to explicitly identify all transformations which are in $\mathrm{Rot}(\Sigma)$. In order to do this we will use two facts about rotations of Σ. First, $\mathrm{Rot}(\Sigma)$ is transitive. That is, for any point $z_0 \in \Sigma$, there is some $T \in \mathrm{Rot}(\Sigma)$ such that $T(z_0) = \infty$. This can be seen visually by realizing that for any point on $\mathbb{S}^2$, there is always a rotation that brings it to the north pole. Second, every element of $\mathrm{Rot}(\Sigma)$ preserves all antipodal points. If $T \in \mathrm{Rot}(\Sigma)$, then T sends every pair of antipodal points in Σ to another pair of antipodal points. This hearkens back to one of the "intuitional pitfalls" as discussed in the Möbius Transformation section. All rigid motions of $\mathbb{S}^2$ preserve antipodal points *on the sphere,* but only pure rotations preserve antipodal points after they are projected back onto the extended complex plane. The proof for the following theorem is taken from [9].

Theorem 9. *A Möbius Transformation T is a rotation of Σ if and only if it is of the form*

$$T(z) = \frac{az+b}{-\bar{b}z+\bar{a}}, \qquad |a|^2+|b|^2 = 1$$

Proof. First, we will show that every rotation of Σ takes on the stated form. Let $p = (X, Y, Z)$ and $p' = (-X, -Y, -Z)$ be a pair of antipodal points on $\mathbb{S}^2$. Recall the explicit formula for the stereographic projection.

$$\pi(X, Y, Z) = \frac{X+iY}{1-Z}$$

Then we have

$$\pi(p) = \frac{X+iY}{1-Z} \qquad \text{and} \qquad \pi(p') = \frac{-X-iY}{1+Z}$$

We can perform some algebraic manipulation on $\pi(p')$ to express it in another form.

$$\pi(p') = -1\left[\frac{X+iY}{1+Z}\right] = -1\left[\frac{X^2+Y^2}{(1+Z)(X-iY)}\right] = -1\left[\frac{(X^2+Y^2)(1-Z)}{(1^2-Z^2)(X-iY)}\right]$$

Now, we know that p is on the surface of $\mathbb{S}^2$ and so

$$X^2+Y^2+Z^2 = 1 \qquad \Rightarrow \qquad X^2+Y^2 = 1-Z^2$$

[8]or $2\pi n$ for any integer n

We can use this to make a substitution in the expression for $\pi(p')$.

$$\pi(p') = -1\left[\frac{(1-Z^2)(1-Z)}{(1-Z^2)(X-iY)}\right] = -1\left[\frac{(1-Z)}{(X-iY)}\right] = -\frac{1}{\overline{\pi(p)}}$$

This tells us that two points, z and z' in Σ map to antipodal points on $\mathbb{S}^2$ if and only if

$$z' = -\frac{1}{\bar{z}}$$

Now, if complex numbers z and z' are antipodal, then we know $T(z)$ and $T(z')$ are antipodal because rotations map antipodal pairs to antipodal pairs. Thus, we have the condition

$$T\Big(-\frac{1}{\bar{z}}\Big) = -\frac{1}{\overline{T(z)}}$$

Now, let a rotation $T(z)$ be given by

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

in such a way that $ad - bc = 1$. Then, applying this condition to T, we have

$$\frac{a(-\frac{1}{\bar{z}})+b}{c(-\frac{1}{\bar{z}})+d} = \frac{b\bar{z}-a}{d\bar{z}-c} = \frac{-\bar{c}\bar{z}-\bar{d}}{\bar{a}\bar{z}+\bar{b}} = -\left(\frac{\bar{a}\bar{z}+\bar{b}}{\bar{c}\bar{z}+\bar{d}}\right)^{-1}$$

Substituting z for $\bar{z}$, we can write the corresponding matrix representations of each side.

$$\begin{bmatrix} b & -a \\ d & -c \end{bmatrix} = \alpha \begin{bmatrix} -\bar{c} & -\bar{d} \\ \bar{a} & \bar{b} \end{bmatrix}$$

$$-bc + ad = \alpha^2(-\overline{cb} + \overline{ad})$$

Since $ad - bc = 1$, we have $\overline{ad} - \overline{bc} = \bar{1} = 1$. This means that $\alpha^2 = 1$ and so $\alpha = \pm 1$.
If $\alpha = 1$, then we have

$$b = -\bar{c}, \quad -c = \bar{b}, \quad a = \bar{d}, \quad d = \bar{a}$$

If $\alpha = -1$, then we have

$$b = \bar{c}, \quad c = \bar{b}, \quad -a = \bar{d}, \quad d = -\bar{a}$$

However, if T is of the form given by this second case, then

$$T = \begin{bmatrix} a & b \\ \bar{b} & -\bar{a} \end{bmatrix}$$

$$\det \begin{bmatrix} a & b \\ \bar{b} & -\bar{a} \end{bmatrix} = -a\bar{a} - b\bar{b} = -|a|^2 - |b|^2 = 1$$

This is clearly impossible and so we must have only the first case where $\alpha = 1$. Thus, every rotation T is of the form

$$T(z) = \frac{az+b}{-\bar{b}z+\bar{a}}, \qquad |a|^2 + |b|^2 = 1 \tag{2}$$

Now, we will show that all transformations of the above form are indeed rotations of Σ. First suppose we have a transformation T of the given form but with $b = 0$. Then,

$$T(z) = \frac{a}{\bar{a}}z = \frac{a^2}{|a|^2}z$$

We observe that the complex number $\frac{a^2}{|a|^2}$ has modulus 1 and so it can be written as $e^{i\theta}$ for some $-\pi \leq \theta \leq \pi$. This gives

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

So T is a rotation of the extended complex plane by and angle of θ about the origin. Thus T is conjugate to a rotation of $\mathbb{S}^2$ by angle θ about the Z axis.
Now, consider another transformation of the given form where b is nonzero.

$$S(z) = \frac{az + b}{-\bar{b}z + \bar{a}}, \qquad |a|^2 + |b|^2 = 1$$

Let $S(0) = z_0$. We know that Rot(Σ) is transitive and so there must be some rotation R such that $R(z_0) = 0$. Then,

$$(R \circ S)(0) = 0$$

Since R is a rotation, it is in the form given by (2) and through direct calculation, we can conclude that $R \circ S$ is in this form as well. But $R \circ S$ also fixes 0 and so it must be given by $(R \circ S)(z) = R_\theta(z) = e^{i\theta}z$ for some $-\pi \leq \theta < \pi$ and $R \circ S \in \text{Rot}(\Sigma)$. This means that we can write S as the compositions of two rotations, $S = R^{-1}R_\theta$, and so S must be a rotation itself. □

Elliptic Transformations and Rotations of the Sphere

Rotations of Σ share some strong similarities with elliptic transformations. In particular, they have two fixed points and all the other points move in circles around these. In fact, all rotations of Σ are elliptic. This can be seen by calculating the trace of the form given in Theorem 9. But the converse is not necessarily true: there are elliptic transformations that do not preserve antipodal points so they cannot be in Rot(Σ). Geometrically, these transformations consist of rotations of $\mathbb{S}^2$ along with translations in the X and Y directions. However, there is a connection we can make between all elliptic transformations and rotations of Σ– and we can use *conjugation* to do so.

Theorem 10. *Any subgroup of* Möb *consisting only of elliptic transformations together with the identity transformation, I, is conjugate to subgroup of Rot(Σ).*

Remark: This proof is also given in [9]. I have broken it into six steps to help the reader digest it.

Proof. **Step 0: Addressing the trivial case**
Let Γ be a subgroup of Möb that contains only elliptic transformations and the identity. If Γ consists only of the identity transformation, then the theorem is trivial since $I \in \text{Rot}(\Sigma)$. So let us assume that $|\Gamma| > 1$.

Step 1: Setting things up
Let T be a non-identity transformation in Γ.

$$T \neq \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

By assumption, T is elliptic and so it has 2 fixed points, z_0 and z_1. Let U be a Möbius Transformation such that

$$U(z_0) = 0 \quad \text{and} \quad U(z_1) = \infty$$

We know that such a transformation exists because of the transitivity of $\mathsf{M\ddot{o}b}$. The conjugate transformation UTU^{-1} is elliptic[9] and its fixed points are 0 and ∞. This means that it must given by a diagonal matrix of the form shown below. Since the transformation is elliptic, we know that $|\lambda| = 1$ and so $\lambda^{-1} = \bar{\lambda}$.

$$U \circ T \circ U^{-1} = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} = \begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix}$$

Now, let Δ be the conjugate group $U\,\Gamma\,U^{-1}$ and let $S \in \Delta$ be $S = U\,T\,U^{-1}$. Choose an arbitrary $F \in \Delta$ where

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

and choose the entries of the matrix so that $ad - bc = 1$.

Step 2: Showing $\bar{a} = d$

First, we will show that for any F, it must be true that $\bar{a} = d$. If $S \in \Delta$ and $F \in \Delta$, then $S \circ F \in \Delta$ since Δ is a group. Thus, $S \circ F$ is elliptic and $\tau(SF)$ is a positive real number.

$$S \circ F = \begin{bmatrix} a\lambda & b\bar{\lambda} \\ c\lambda & d\bar{\lambda} \end{bmatrix}$$

$$a\lambda + d\bar{\lambda} \in \mathbb{R} \quad \Rightarrow \quad d\bar{\lambda} - \overline{a\lambda} \in \mathbb{R} \quad \Rightarrow \quad \bar{\lambda}(d - \bar{a}) \in \mathbb{R}$$

Now, $|\lambda| = 1$ but we know that $\lambda \neq \pm 1$ and so we can be certain $\bar{\lambda} \notin \mathbb{R}$. This means that for the above statement to be true we must have $d - \bar{a} = 0$ and so $d = \bar{a}$. Hence, every $F \in \Delta$ is of the form

$$F = \begin{bmatrix} a & b \\ c & \bar{a} \end{bmatrix} \tag{3}$$

Step 3: Addressing the case where $b = 0$

Now, we will show that $b = 0$ if and only if $c = 0$. First, assume that $c = 0$. Then we have

$$F = \begin{bmatrix} a & b \\ 0 & \bar{a} \end{bmatrix}$$

Since we are assuming that $ad - bc = 1$, we can conclude that for an F of this form, $a\bar{a} = |a|^2 = 1$. Now, we know that $SFS^{-1}F^{-1} \in \Delta$ by group properties, and we can perform matrix multiplication to find the coefficients of this transformation.

$$SFS^{-1}F^{-1} = \begin{bmatrix} 1 & ba(\lambda^2 - 1) \\ 0 & 1 \end{bmatrix}$$

Notice that $\tau(SFS^{-1}F^{-1}) = 4$. Since this cannot be a parabolic transformation, we must conclude that it is the identity and $ba(\lambda^2 - 1) = 0$. Again, we know that $\lambda \neq \pm 1$ and so $\lambda^2 - 1 \neq 0$, implying that $ba = 0$. If $a = 0$, then F would not be invertible and so we have $b = 0$.

[9] Conjugate transformations have the same value for τ and thus are part of the same class of transformations

The argument for the other direction can be done in the same way.

Step 4: Showing there is a single r such that $c = r\bar{b}$ for every transformation
Now, we consider the case when F is of the form (3) with $b \neq 0 \neq c$.

$$F = \begin{bmatrix} a & b \\ c & \bar{a} \end{bmatrix}$$

Let $r = c/\bar{b}$ and write c as $r\bar{b}$. Then, we have

$$a\bar{a} - bc = 1 = a\bar{a} - b\bar{b}r = |a|^2 - r|b|^2 = 1$$

Thus, we see that $r \in \mathbb{R}$. Now, consider two different transformations, $F_1, F_2 \in \Delta$ that are written in this form. (Assuming $b_1 \neq 0 \neq b_2$).

$$F_1 = \begin{bmatrix} a_1 & b_1 \\ r_1\overline{b_1} & \overline{a_1} \end{bmatrix} \qquad F_2 = \begin{bmatrix} a_2 & b_2 \\ r_2\overline{b_2} & \overline{a_2} \end{bmatrix}$$

We know that $F_1 \circ F_2 \in \Delta$ and so it is elliptic and has a real trace.

$$F_1 \circ F_2 = \begin{bmatrix} a_1 & b_1 \\ r_1\overline{b_1} & \overline{a_1} \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ r_2\overline{b_2} & \overline{a_2} \end{bmatrix} = \begin{bmatrix} a_1a_2 + r_2b_1\overline{b_2} & * \\ * & \overline{a_1a_2} + r_1\overline{b_1}b_2 \end{bmatrix}$$

$$a_1a_2 + r_2b_1\overline{b_2} + \overline{a_1a_2} + r_1\overline{b_1}b_2 \in \mathbb{R}$$

Since $a_1a_2 + \overline{a_1a_2} \in \mathbb{R}$, we conclude that $r_2b_1\overline{b_2} + r_1\overline{b_1}b_2 \in \mathbb{R}$. The real parts of these terms are the same and so they must be complex conjugates.

$$r_1\overline{b_1}b_2 = r_2\overline{b_1}b_2$$

Thus, $r_1 = r_2$. This means that the choice for r is independent of the element of Δ and so we can choose the same value of r for every element in Δ. (If Δ consists of only diagonal matrices, then any arbitrary value for r will work.)

Step 5: Defining a new transformation based on r
Let $v = |r|^{\frac{1}{4}}$ and define the transformation V to be

$$V = \begin{bmatrix} v & 0 \\ 0 & v^{-1} \end{bmatrix}$$

Notice that $V \circ S \circ V^{-1} = S$. In other words, all diagonal matrices are unchanged after conjugation by V. Now, consider what happens when we conjugate an arbitrary transformation by V.

$$VFV^{-1} = \begin{bmatrix} v & 0 \\ 0 & v^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ r\bar{b} & \bar{a} \end{bmatrix} \begin{bmatrix} v^{-1} & 0 \\ 0 & v \end{bmatrix}$$

$$= \begin{bmatrix} a & b|r|^{\frac{1}{4}} \\ |r|^{-\frac{1}{2}} \cdot r\bar{b} & \bar{a} \end{bmatrix}$$

Depending on the sign of r, we have two possibilities for the form of VFV^{-1}.

$$VFV^{-1} = \begin{cases} \begin{bmatrix} a & b|r|^{\frac{1}{4}} \\ |r|^{\frac{1}{2}}\overline{b} & \overline{a} \end{bmatrix} & r > 0 \quad (i) \\ \\ \begin{bmatrix} a & b|r|^{\frac{1}{4}} \\ -|r|^{\frac{1}{2}}\overline{b} & \overline{a} \end{bmatrix} & r < 0 \quad (ii) \end{cases}$$

Step 6: Reducing the possibilities
Note that the subgroup $V\Delta V^{-1} = VU\Gamma U^{-1}V^{-1}$ still consists of only elliptic transformations together with the identity. If we have a transformation $G \in V\Delta V^{-1}$ of type (i), then by direct calculation we find $\tau(SGS^{-1}G^{-1}) > 4$. Thus, the transformation is not elliptic and so every transformation in $(VU)\Gamma(VU)^{-1}$ is of type (ii).

$$T = \begin{bmatrix} a & b|r|^{\frac{1}{4}} \\ -|r|^{\frac{1}{2}}\overline{b} & \overline{a} \end{bmatrix}$$

This matrix is in the form stated in Theorem 9. Hence, if $T \in (VU)\Gamma(VU)^{-1}$, then T is a rotation and Γ is conjugate to a subgroup of $\mathrm{Rot}(\Sigma)$. □

On its own, this is an extremely fascinating result; one that I have enjoyed attempting to wrap by head around. But the real beauty of this theorem appears when we take it one step further.

Lemma 2. *All finite subgroups of* Möb *consist only of elliptic transformations and the identity, I.*

Proof. Suppose that Γ is a subgroup of Möb and that there is some $T \in \Gamma$ such that T is not elliptic. Then, by definition of a group, we have

$$T^k \in \Gamma \qquad \text{for every positive integer } k$$

Since T is not elliptic, it cannot have a finite period. This means that if $k \neq m$, then $T^k \neq T^m$. Γ must contain all orders of compositions of T and thus infinitely many elements. Hence, Γ is not finite. □

Remark: It is not true that every subgroup of Möb consisting entirely of elliptic transformations is finite. In order for a group of elliptic transformations to be finite, each transformation in the group must have a finite period.

Combining Theorem 10 and Lemma 2, we can have the following statement.

Corollary 2. *If Γ is a finite subgroup of* Möb *, then Γ is conjugate a subgroup of Rot(Σ).*

In the next section, we shall see that finite subgroups of Möb hold some very interesting properties, but we have one more connection to make before we can reveal the big result.

Lemma 3. *The rotation group of Σ, Rot(Σ), is isomorphic to the rotation group of $\mathbb{R}^3$, $SO(3)$.*

Proof. Recall that we defined $T \in \mathrm{Rot}(\Sigma)$ to be conjugate to a rotation Φ of $\mathbb{S}^2$ under stereographic projection. Every rotation in $SO(3)$ can be completely determined by a rotation of the unit sphere. We can define a map f by

$$f : \mathrm{Rot}(\Sigma) \to SO(3) \qquad f(T) = \pi^{-1} \circ T \circ \pi = \Phi$$

Suppose that $T, S \in \mathrm{Rot}(\Sigma)$. Then we have

$$f(TS) = \pi^{-1} \circ (TS) \circ \pi = (\pi^{-1} \circ T \circ \pi)(\pi^{-1} \circ S \circ \pi) = f(T) \circ f(S)$$

So f is a group homomorphism. Also, since π is a bijection, this map must also be a bijection. Thus, the two groups are isomorphic. $\square$

Finite Subgroups of Möbius Transformations

A Beautiful Result

Finite subgroups of $PSL(2, \mathbb{C})$ are known as **Kleinian groups**. These groups are related to finite subgroups of $\mathsf{M\ddot{o}b}$ – and consequently finite subgroups of $SO(3)$– as we have dicussed. Each Möbius Transformations corresponds to two matrices with determinant 1. Kleinian groups are a well-studied subject in group theory. The following theorem addresses the structure of finite subgroups of $SO(3)$ and comes to a very nice conclusion. These ideas were first studied by Felix Klein and Henri Poincaré in 1883 and the following proof was published by Klein in *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* in 1888 (*Lectures on the Icosahedron and the Resolution of Equations of Degree Five*)[10]. The proof that I will give follows that of Jones and Singerman in *Complex Functions* [9], and Chan in his video *Finite Subgroups of SO(3)* [5], but the core ideas are those presented by Klein.

Theorem 11. *Let Γ be a finite subgroup of $SO(3)$. Then one of the following is true:*

1. *Γ is cyclic*
2. *Γ is dihedral*
3. *Γ is the rotational symmetry group of a platonic solid*
   (i.e. the tetrahedron, cube/octahedron, or dodecahedron/icosahedron)

Proof. We will approach this proof in two parts. In the first, we will find all the possibilities for the numbers and sizes of orbits in the fixed point set of a subgroup Γ. In the second part, we will take each possibility and use the characterization of the orbits to construct one of the symmetry groups stated in the theorem. This second part we will not do rigorously, but I will give the reader intuition for why it must be true. If the reader wishes to see a rigorous proof, I direct them towards *Complex Functions* [9].

We will start with some basic setup for the proof. Let Γ be a finite subgroup of $SO(3)$ and let X be the fixed point set of Γ. That is, if $x \in X$, then there is some non-identity $T \in \Gamma$ such that $T(x) = x$. Any element of Γ must send every fixed point to another fixed point. To see this, notice that for every $x \in X$, we know $|\text{Stab}(x)| \geq 2$ [10]. And for any $y \notin X$, $|\text{Stab}(y)| = |\{I\}| = 1$. Now, from Corollary 1 we have that for every $x \in \Gamma$,

$$|\Gamma| = |\text{Stab}(x)| \cdot |\Omega_x|$$

This tells us that if two elements are in the same orbit, then they must have the same size stabilizer. Hence, a fixed point and a non-fixed point cannot have the same size stabilizer and so they are not in the same orbit.

As we have just shown, elements in the same orbit have the same size stabilizers. Let

$$e_i = |\text{Stab}(x_i)| = |\text{Stab}(T(x_i))|$$

so that the set $\{e_1, e_2, ...e_r\}$ is the set of the sizes of stabilizers corresponding to each of the r orbits. We can rearrange this set in ascending order so that

$$e_1 \leq e_2 \leq ... \leq e_r$$

[10] The stabilizer contains at least one other element besides the identity.

As a last statement for the setup, for each $1 \leq i \leq r$, we have the inequality

$$\frac{1}{2} \leq 1 - \frac{1}{e_i} \leq 1 \tag{4}$$

This is simply because we know $e_i \geq 2$ for every i. This last statement seems out of the blue right now, but it will be useful later.

Part I: Describing the Possible Orbits

Recall Burnside's Lemma (Theorem 6) as we discussed in the group theory section. Let $r = |X/\Gamma|$ be the number of orbits in X and $|X^T|$ be the number of points in X fixed by $T \in \Gamma$.

$$r = \frac{1}{|\Gamma|} \sum_{T \in \Gamma} |X^T|$$

This gives us an expression for the number of orbits– a first step in characterizing the possible orbits in X. Let $N = |\Gamma|$ for brevity moving forward.

$$r = \frac{1}{N}\left[|X^I| + \sum_{T \in (\Gamma - \{I\})} |X^T|\right]$$

Here we have simply separated out the identity in the sum because it is a special case. Now, we can write an explicit expression for this new sum. Each non-identity element in Γ is a rotation about an axis and so it fixes two points. There are $N-1$ elements in $\Gamma - \{I\}$ and so we can rewrite the sum as $2(N-1)$. Also, the identity fixes every point so $|X^I| = |X|$.

$$r = \frac{1}{N}\left[|X| + 2(N-1)\right]$$

Each orbit in X is disjoint and so the size of X is the sum of the sizes of the orbits. If e_i is the size of the stabilizer for elements in Ω_i, then $|\Omega_i| = N/e_i$ because of Corollary 1. Applying this to our expression for r, we have

$$r = \frac{1}{N}\left[\sum_1^r \frac{N}{e_i} + 2N - 2\right]$$

$$r = \sum_1^r \frac{1}{e_i} + 2 - \frac{2}{N}$$

And now, for convenience, we will write r as $\sum_1^r 1$ and move the other sum to the left hand side to combine them.

$$\sum_1^r \left(1 - \frac{1}{e_i}\right) = 2 - \frac{2}{N} \tag{5}$$

Now, we can find the number of orbits. Applying (4) to this expression, we have

$$\frac{r}{2} \leq \sum_1^r \left(1 - \frac{1}{e_i}\right) = 2 - \frac{2}{N} < 2$$

Suppose that $r \geq 4$. Then we have

$$\frac{4}{2} = 2 \leq \frac{r}{2} \leq 2 - \frac{2}{N} < 2$$

But this gives us the strict inequality $2 < 2$ which is a false statement. And so the original supposition was false and $r \leq 3$. Now, suppose that $r = 1$. Then

$$1 > 1 - \frac{1}{e_1} = 2 - \frac{2}{N}$$

and we have

$$\begin{aligned} 1 &> 2 - \frac{2}{N} \\ \frac{1}{2} &> 1 - \frac{1}{N} \end{aligned}$$

This means that we must have $N = 1$ and Γ is the trivial group. Γ can be considered to be the cyclic group of size 1, so it affirms the claim. However, this is a rather uninteresting case.

Let us now consider when $r = 2$ or $r = 3$. First, suppose that $r = 2$. Then (5) becomes

$$\begin{aligned} 1 - \frac{1}{e_1} + 1 - \frac{1}{e_2} &= 2 - \frac{2}{N} \\ \frac{1}{e_1} + \frac{1}{e_2} &= \frac{2}{N} \\ \frac{N}{e_1} + \frac{N}{e_2} &= 2 \\ |\Omega_1| + |\Omega_2| &= 2 \end{aligned}$$

And since the sizes of orbits must be positive integers, we know that

$$|\Omega_1| = |\Omega_2| = 1$$

So Γ is a finite subgroup of rotations with two fixed points. This is the case where Γ is cyclic as we shall see in Part II.

Now suppose that $r = 3$. In this case, (5) gives

$$\begin{aligned} 3 - \frac{1}{e_1} - \frac{1}{e_2} - \frac{1}{e_3} &= 2 - \frac{2}{N} \\ \frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} &= 1 + \frac{2}{N} \end{aligned}$$

In particular, notice that the value on the right-hand side is strictly larger than 1 and so the left-hand must also be larger than 1. Recall that we have arranged e_1, e_2, e_3 in *ascending order*. If $e_1 \geq 3$, then $e_2 \geq 3$ and $e_3 \geq 3$ as well. If this is true, then

$$\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} \leq \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$$

However, we know that this expression must be strictly greater than 1 so we conclude that this case is impossible and $e_1 = 2$. If $e_2 \geq 4$, then $e_3 \geq 4$ as well. But then we have

$$\frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} \leq \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1$$

This again produces a contradiction and so we know that $e_2 = 2$ or $e_2 = 3$. These conditions give four different possibilities for the sizes of the three stabilizers.

$$(2, 2, n)$$

For this case, (5) becomes $\frac{1}{2} + \frac{1}{2} + \frac{1}{n} = 1 + \frac{2}{N}$ and so we then have $N = 2n$. We will later see that this option corresponds to the dihedral group D_{2n}.

$$(2, 3, 3)$$

With this option, we have $\frac{1}{2} + \frac{1}{3} + \frac{1}{3} = \frac{7}{6} = 1 + \frac{2}{N}$. So in this case we have $N = 12$. This option is the symmetry group of the tetrahedron.

$$(2, 3, 4)$$

Here we have $\frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{13}{12} = 1 + \frac{2}{N}$. This gives us that $N = 24$. In this case, Γ is the symmetry group of both the cube and the octahedron.

$$(2, 3, 5)$$

Finally, this case gives $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} = \frac{31}{30} = 1 + \frac{2}{N}$. Here, we see $N = 60$. This is the symmetry group of the dodecahedron and the icosahedron.

Now, we ask if the sizes of the stabilizers could possibly be $(2, 3, 6)$. Well notice that

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$$

And so 5 is the upper bound for the size of the third stabilizer.

Part II: Constructing the Groups

Now, we turn towards the construction of the corresponding groups. First, let us consider the only case with two orbits. This possibility is a cyclic group of order N. Recall that we deduced each orbit in X has one element.

$$|\Omega_1| = |\Omega_2| = 1$$

This means that Γ has two fixed points. Since every element in Γ is a rotation– and the fixed points of a rotation are antipodal– for each $x \in X$, there is also an $x' \in X$ such that x and x' are antipodal. Γ has only two fixed points so they must be antipodal. Hence, every $R \in \Gamma$ must be about the same axis. Now, let R_φ be the element in Γ with the smallest angle of rotation. I claim that R_φ must generate Γ. For contradiction, suppose it did not. Then there is some $R_\theta \in \Gamma$ such that $n\varphi \neq \theta$ for all $n \in \mathbb{Z}$. This means θ is between some $m\varphi$ and $(m+1)\varphi$ (see Figure 6). But then, because Γ is a group, we know that $R_{\theta - m\varphi} \in \Gamma$ as well. Notice that $\theta - m\varphi < \varphi$ and so now we have a contradiction since we took φ to be the smallest angle of rotation. This tells us that Γ has a generator, R_φ, and so Γ is cyclic.

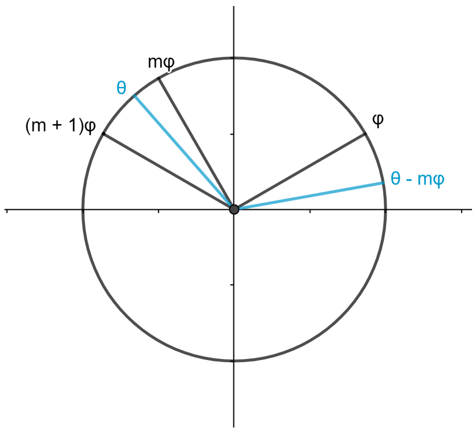


Figure 6

Now, we turn our attention to the possibilities for three orbits in X. To give a rigorous argument for the following parts of the theorem, one could use the fact that every $g \in \Gamma$ sends fixed points to other fixed points. Then, by systematically examining the orbit of each fixed point, it follows that the fixed points must be evenly spaced in such a way that Γ is the stated symmetry group. I will not give this argument, but rather I will explain using visual and intuitional means why these symmetry groups appear.

$(\mathbf{2}, \mathbf{2}, \mathbf{n})$

First, we will look when the sizes of the stabilizers are given by $(2, 2, n)$. Here, $|\Gamma| = 2n$. We can find the sizes of the corresponding orbits by applying Corollary 1.

$$|\Omega_1| = \frac{2n}{2} = n \qquad |\Omega_2| = \frac{2n}{2} = n \qquad |\Omega_3| = \frac{2n}{n} = 2$$

In this case, Γ is the symmetry group of the regular n-gon that lies at the equator of the sphere. Figure 7 shows an example of this with a square. This is the same as the symmetry group of an n-gon in two dimensions, D_{2n}. The rotational symmetry group of this shape consists of n rotations about the Z axis, and n $180°$ rotations– one for each axis that passes through a vertex/midpoint of an edge.

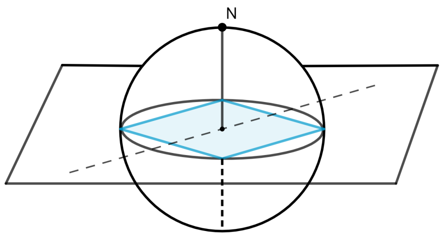


Figure 7

One orbit of length n corresponds to the vertices of the polygon, and the other to the midpoints of the edges. Each rotation around the Z axis by an angle of $\frac{2\pi}{n}$ will map vertices to vertices and edges to edges. There are n of these rotations (including the identity), and so the edges and vertices both have an orbit size of n. Each of these points has a stabilizer of 2 consisting of the identity and a rotation about the axis of symmetry that passes through it.

The orbit of size 2 corresponds to the north and south pole. These points are fixed by the n rotations about the Z axis and so their stabilizer has size n. Each rotation around an axis through a vertex/edge will permute the north and south pole.

$(\mathbf{2}, \mathbf{3}, \mathbf{3})$

This case gives the symmetry group of the tetrahedron and its platonic dual– which also happens to be the tetrahedron. Here, we have $|\Gamma| = 12$. The sizes of the orbits are as follows:

$$|\Omega_1| = \frac{12}{2} = 6 \qquad |\Omega_2| = \frac{12}{3} = 4 \qquad |\Omega_3| = \frac{12}{3} = 4$$

The set of 4 vertices corresponds to Ω_2 and the set of 4 faces corresponds to Ω_3[11]. Notice that an axis of symmetry through a vertex passes through the midpoint of a face on the other side. This means that a face and its opposite vertex have the same stabilizer. Looking at the tetrahedron from the perspective of one of these axis, we see that it has three-fold rotational symmetry. Thus, both the faces and the vertices have a stabilizer of size 3.
The set of fixed points at the midpoint of the 6 edges corresponds with Ω_1. Notice that an axis of symmetry passing through the midpoint of an edge passes through another edge on the other side. Looking at the tetrahedron from the perspective of this axis, it only has two-fold symmetry and so the size of the stabilizer of an edge is 2.

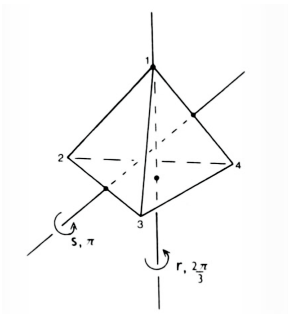
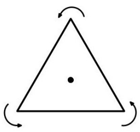
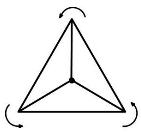


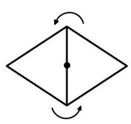
Figure 8



Point of view from face



Point of view from vertex



Point of view from edge

[11] This is an arbitrary choice. The set of vertices could correspond to Ω_3 and vice versa.

(2, 3, 4)

This possibility describes the symmetry group of both the cube and the octahedron. Since they are platonic duals, they have the same symmetry group. Here, we will think about the symmetry group of the cube, but it follows much the same way for the octahedron. In this case, $|\Gamma| = 24$.

$$|\Omega_1| = \frac{24}{2} = 12 \qquad |\Omega_2| = \frac{24}{3} = 8 \qquad |\Omega_3| = \frac{24}{4} = 6$$

The 6 faces of the cube correspond to Ω_3. If we look at the cube from the perspective of an axis through the midpoint of a face, we see that it has four-fold rotational symmetry. Thus, the size of the stabilizer of each face is 4.
There are 8 vertices on a cube, so the fixed points corresponding to the vertices are given by Ω_2. From the perspective of an axis through a vertex, the cube has three-fold symmetry. Thus, the stabilizers of these points have size 3.
Lastly, the set of fixed points at the midpoint of each of the 12 edges corresponds to Ω_1. When the cube is seen from the perspective of this axis, it has two-fold symmetry. So these fixed points have a stabilizer size of 2.

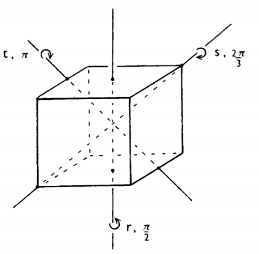
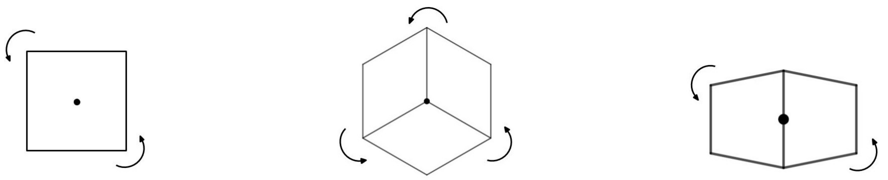


Figure 9



Point of view from face Point of view from vertex Point of view from edge

$(\mathbf{2},\mathbf{3},\mathbf{5})$

The last possibility describes the symmetry group of the dodecahedron and the icosahedron. Again, these are platonic duals and so they have the same symmetry group. Here, we will examine the group structure of the dodecahedron. In this case, $|\Gamma| = 60$.

$$|\Omega_1| = \frac{60}{2} = 30 \qquad |\Omega_2| = \frac{60}{3} = 20 \qquad |\Omega_3| = \frac{60}{5} = 12$$

First, the fixed points on the 12 faces appear in Ω_3. An axis through the midpoint of a face intersects another face on the other side. From the perspective of this axis, the dodecahedron has five-fold symmetry so the faces have a stabilizer of size 5.
The set of vertices correspond to Ω_2 since there are 20 vertices. An axis of symmetry through a vertex passes through another vertex on the other side. From the perspective of this axis, there is three-fold symmetry and so the vertices have a stabilizer of size 3.
Finally there are 30 edges in the dodecahedron so Ω_3 corresponds to the set of midpoints of edges. Looking at the dodecahedron from the perspective of one of these fixed points, we have two-fold rotational symmetry so the edges have a stabilizer size of 2.

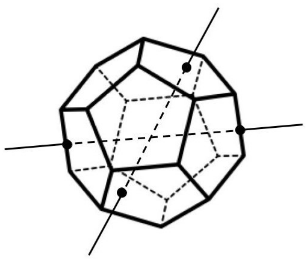
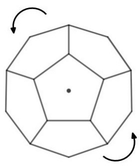
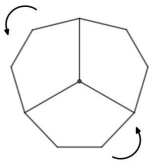


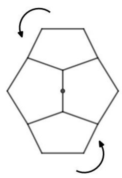
Figure 10



Point of view from face



Point of view from vertex



Point of view from edge

□

And finally, we have come to the amazing conclusion. We have shown that every finite subgroup of $\mathsf{M\ddot{o}b}$ is conjugate to a subgroup of $\mathrm{Rot}(\Sigma)$ (Corollary 2) and we have shown that $\mathrm{Rot}(\Sigma)$ is isomorphic to $SO(3)$ (Lemma 3). These results paired with our characterization of finite subgroups of $SO(3)$ (Theorem 11) gives the following result.

Corollary 3. *Every finite subgroup of* $\mathsf{M\ddot{o}b}$ *is isomorphic (through conjugation) to one of the following:*

1. *A cyclic group*
2. *A dihedral group (D_{2n})*
3. *The rotational symmetry group of a platonic solid*

Implications

Möbius Transformations and complex analysis tend to be very "continuous" fields in math, whereas the platonic solids and symmetry groups are very "discrete". The collision of these two spheres of mathematics often produces beautiful results. Conceptualizing Möbius Transformations through stereographic projection and relating them to the unit sphere has given us a bridge between the continuous and the discrete. Using group theory concepts of conjugation, we were able to divide $\mathsf{M\ddot{o}b}$ into conjugacy classes. This allowed us to characterize rotations of Σ and all finite subgroups of $\mathsf{M\ddot{o}b}$. Then, linking $\mathrm{Rot}(\Sigma)$ to $SO(3)$, we were able to use results from group theory to reveal the symmetries of finite Möbius groups.

I find this result extremely surprising and beautiful. When I began an investigation to understand subgroups of Möbius Transformations, I was not expecting the platonic solids to appear– and yet, these shapes do have a habit of showing up in surprising places. The connection between Möbius Transformations and the platonic solids suggests that finite subgroups of $\mathsf{M\ddot{o}b}$ must contain some specific symmetries. It seems that a subgroup of $\mathsf{M\ddot{o}b}$ generated by *any* finite set of Elliptic transformations with finite period may not turn out to be finite. The transformations that generate a finite group must have fixed points that are in some way symmetric. I do not completely understand the implications of this result, but I plan on continuing to seek answers.

I am also interested in some other questions. Are there as beautiful results as these when we consider infinite groups? How do Kleinian groups and surrounding research fit into this investigation? Can these ideas be extended to higher dimensions? I am looking forward to embarking on another expedition.

References

[1] Lars V. Ahlfors. Finitely Generated Kleinian Groups. *American Journal of Mathematics*, 86(2):413–429, 1964.

[2] Paolo Aluffi. *Algebra: Chapter 0*, volume 104. American Mathematical Soc., 2009.

[3] James W Anderson. *Hyperbolic Geometry.* Springer Science & Business Media, 2006.

[4] Douglas Arnold and Jonathan Rogness. *Möbius Transfomrations Revealed.* Jun 2007.

[5] Daniel Chan. *Classification of the Finite Subgroups of SO(3).* DanielChanMaths, July 2018.

[6] Theodore Gamelin. *Complex Analysis.* Springer Science & Business Media, 2003.

[7] Michael Harrison, Kimberly Harrison, and Liliana de Castro. *Cosets and Lagrange's Theorem - The Size of Subgroups (Abstract Algebra).* Socratica, Mar 2017.

[8] Michael P Hitchman. *Geometry with an Introduction to Cosmic Topology.* Jones & Bartlett Learning, 2009.

[9] Gareth A. Jones and David Singerman. *Complex Functions: An Algebraic and Geometric Viewpoint*, chapter 2. Cambridge University Press, 1987.

[10] F. Klein. *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* London : Trubner C, 1888.

[11] R. C. Lyndon and J. L. Ullman. Groups of Elliptic Linear Fractional Transformations. *Proceedings of the American Mathematical Society*, 18(6):1119–1124, 1967.

[12] Tristan Needham. *Visual Complex Analysis.* Oxford University Press, 1998.

[13] John Olsen. The Geometry of Möbius Transformations. *Rochester: University of Rochester*, 2010.