Notre Dame 2025 Undergraduate Thematic Program in Discrete Groups in Topology and Algebraic Geometry

June 2025

Abstract

Notes from Notre Dame 2025 Undergraduate Thematic Program on discrete groups in topology and algebraic geometry through the lens of elliptic curves, their moduli, and connections with basic principles of geometric group theory.

Lectures given by Daniel Studenmund (Binghamton University), Nicholas Salter (University of Notre Dame), and Shuddhodan Kadattur Vasudevan (University of Notre Dame).

This is an unofficial set of notes scribed by Gary Hu, who is responsible for all mistakes. If you find any errors, please report them to: gh7@williams.edu

Contents

1 Monday, June 2

1.1 AM Session 1: Group Actions

An action of a group G on a set X provides a way to understand G as a collection of transformations of X. More formally:

Definition 1.1. *An **action** of a group G on a set X is a homomorphism*

$$\rho : G \to \mathrm{Sym}(X),$$

where $\mathrm{Sym}(X)$ *is the group of all bijections from X to itself.*

We often write $G \circlearrowright X$ to denote that G acts on X. For an element $g \in G$, its image $\rho(g)$ is a bijection on X. For any $x \in X$, we denote the image of x under this bijection by $g \cdot x$, so that $g \cdot x := (\rho(g))(x)$. The homomorphism property $\rho(gh) = \rho(g) \circ \rho(h)$ translates to $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$. The identity element $\mathrm{id} \in G$ maps to the identity map on X, so $\mathrm{id} \cdot x = x$.

Often, the set X is endowed with additional structure, such as a metric, a vector space, a graph, a variety, etc. In these contexts, we are typically interested in actions that preserve this structure. For example, if (X, d) is a metric space, a group action is by isometries if $d(g \cdot x, g \cdot y) = d(x, y)$ for all $x, y \in X$ and $g \in G$. In such cases, the action is given by a homomorphism $G \to \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ is the group of structure-preserving automorphisms of X.

Definition 1.2. *Given an action $G \circlearrowright X$:*

- *The **orbit** of an element $x \in X$ is $G{\cdot}x = \{y \in X \mid y = g{\cdot}x \text{ for some } g \in G\}$.*
- *The **stabilizer** of an element $x \in X$ is $G_x = \{g \in G \mid g \cdot x = x\}$.*
- *The action is **free** if $G_x = \{id\}$ for all $x \in X$, where id is the identity element in G.*
- *The action is **transitive** if $G \cdot x = X$ for any (and thus every) $x \in X$.*

Example 1.3.

- *The symmetric group S_n acts on the set $\{1, 2, \ldots, n\}$. This action preserves the set structure. It is free if $n \leqslant 1$ (only the identity permutation fixes elements if $n = 1$). It is not free if $n \geqslant 2$. The action is transitive if $n \geqslant 1$.*
- *The general linear group $GL_n(k)$ acts on the vector space k^n. This action preserves the vector space structure. The action is free on $k^n \backslash \{0\}$ (the set of non-zero vectors). It is transitive on $k^n \backslash \{0\}$. (It's not free on k^n because the zero vector is fixed by all elements, and not transitive on k^n unless $k^n = \{0\}$).*
- *A group G acts on its Cayley graph $Cay(G, S)$ by left multiplication. This action preserves the graph structure. It is free and transitive.*

- *The special orthogonal group $SO(n)$ acts on the $(n-1)$-sphere S^{n-1}. This action preserves the metric structure of the sphere. The action is transitive. It is not free for $n > 1$ (e.g., rotations fixing a point).*
- *A group G acts on itself by conjugation: $g \cdot h = ghg^{-1}$. This action preserves the group structure (it's an action by automorphisms). The action is free if and only if G is trivial or $G \cong \mathbb{Z}_2$. The action is transitive only if G is trivial or $G \cong \mathbb{Z}_2$.*
- *The fundamental group $\pi_1(X, x_0)$ acts on the universal cover $\tilde{X}$ via deck transformations. This action preserves the topological structure. The action is free. It is generally not transitive (unless $\tilde{X}$ is a point, i.e., X is simply connected, or if $\tilde{X}$ has only one sheet over each point in X for which $\pi_1(X, x_0)$ acts transitively, which implies $\pi_1(X, x_0)$ is trivial or X is path-connected and $\tilde{X}$ is a single point).*

1.2 AM Session 2: Hyperbolic Geometry

Euclidean geometry is characterized by Playfair's axiom, which asserts that for any given line and a point not on the line, there is exactly one line through the point parallel to the given line. For centuries, this was suspected to be a theorem derivable from Euclid's other axioms. The discovery that one can construct a consistent geometry by assuming instead that there are infinitely many such parallels gave birth to hyperbolic geometry.

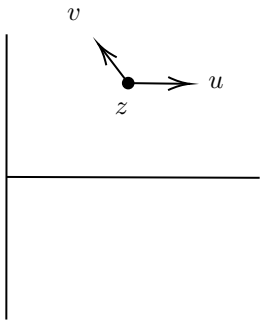
A standard model for hyperbolic geometry is the Poincaré upper half-plane, defined as

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

At each point $z \in \mathbb{H}$, the tangent space $T_z\mathbb{H}$ is a copy of $\mathbb{R}^2$. We endow $\mathbb{H}$ with a Riemannian metric by defining an inner product on each tangent space. For $u, v \in T_z\mathbb{H}$, the inner product is given by

$$\langle u, v \rangle_z = \frac{1}{(\mathrm{Im}(z))^2} \langle u, v \rangle_{\mathbb{R}^2},$$

where $\langle \cdot, \cdot \rangle_{\mathbb{R}^2}$ is the standard Euclidean inner product.



Definition 1.4. *The **hyperbolic length** of a smooth curve $\gamma : [T_0, T_1] \to \mathbb{H}$ is defined as*

$$L_{\mathbb{H}}(\gamma) := \int_{T_0}^{T_1} \sqrt{\langle \dot{\gamma}(t), \dot{\gamma}(t) \rangle_{\gamma(t)}}\, dt = \int_{T_0}^{T_1} \frac{|\dot{\gamma}(t)|_{\mathbb{R}^2}}{\mathrm{Im}(\gamma(t))}\, dt.$$

Exercise 1.5. *Given $0 < a < b$, where $a, b \in \mathbb{R}$, define the curve*

$$\begin{aligned} \gamma : [\log a, \log b] &\to \mathbb{H} \\ t &\mapsto ie^t. \end{aligned}$$

Compute $L_{\mathbb{H}}(\gamma)$.

Solution. We have $\dot{\gamma}(t) = ie^t$. The imaginary part of $\gamma(t)$ is $\mathrm{Im}(\gamma(t)) = e^t$. Thus, $\langle \dot{\gamma}(t), \dot{\gamma}(t) \rangle_{\gamma(t)} = \frac{1}{(\mathrm{Im}(\gamma(t)))^2} \langle ie^t, ie^t \rangle_{\mathbb{R}^2} = \frac{1}{(e^t)^2}(e^t)^2 = 1$.

$$\begin{aligned} L_{\mathbb{H}}(\gamma) &= \int_{\log a}^{\log b} \sqrt{1}\, dt \\ &= \int_{\log a}^{\log b} 1\, dt \\ &= [\mathrm{t}]_{\log a}^{\log b} \\ &= \log(b) - \log(a). \end{aligned}$$

□

Definition 1.6. *The **hyperbolic metric** $d_{\mathbb{H}}$ on $\mathbb{H}$ is the distance function induced by the Riemannian metric. For any two points $z_1, z_2 \in \mathbb{H}$, their distance is the infimum of the lengths of all smooth curves connecting them:*

$$d_{\mathbb{H}}(z_1, z_2) = \inf\{L_{\mathbb{H}}(\gamma) \mid \gamma \text{ is a smooth curve from } z_1 \text{ to } z_2\}.$$

Definition 1.7. *A **geodesic** in a metric space (X, d) is a curve $\gamma : I \to X$, where I is an interval in $\mathbb{R}$, such that*

$$d(\gamma(s), \gamma(t)) = |s - t|$$

for all $s, t \in I$.

Remark 1.8. *This condition implies that γ is parameterized by arc length*

Exercise 1.9. *Show that the curve $\gamma(t) = ie^t$ from the previous exercise, reparameterized appropriately, is a geodesic.*

Definition 1.10. *A **Riemannian isometry** of $\mathbb{H}$ is a diffeomorphism $f : \mathbb{H} \to \mathbb{H}$ that preserves the Riemannian metric. That is, for every $z \in \mathbb{H}$ and all tangent vectors $u, v \in T_z\mathbb{H}$,*

$$\langle D_z f(u), D_z f(v) \rangle_{f(z)} = \langle u, v \rangle_z,$$

where $D_z f$ is the differential (or Jacobian matrix) of f at z.

Theorem 1.11. *A map $f : \mathbb{H} \to \mathbb{H}$ is a Riemannian isometry if and only if it is a metric isometry, i.e., $d_{\mathbb{H}}(f(z_1), f(z_2)) = d_{\mathbb{H}}(z_1, z_2)$ for all $z_1, z_2 \in \mathbb{H}$.*

Remark 1.12. *The implication that a Riemannian isometry is a metric isometry is direct: such a map preserves the lengths of all curves, and therefore preserves the infimal length between any two points. The converse is a deeper result of Riemannian geometry (the Myers-Steenrod theorem).*

The group of orientation-preserving isometries of $\mathbb{H}$ has a particularly elegant description.

Definition 1.13. *The **special linear group** $\mathrm{SL}(2, \mathbb{R})$ is the group of 2×2 real matrices with determinant 1:*

$$\mathrm{SL}(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{R}) \mid ad - bc = 1 \right\}.$$

Proposition 1.14. *The group $\mathrm{SL}(2, \mathbb{R})$ acts on $\mathbb{H}$ by Möbius transformations: for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$ and $z \in \mathbb{H}$, the action is defined by*

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

Furthermore, this action is by orientation-preserving Riemannian isometries.

Sketch of proof. One first verifies that this is a valid group action and that for any $A \in \mathrm{SL}(2, \mathbb{R})$, the map $z \mapsto A \cdot z$ is a bijection from $\mathbb{H}$ to itself. The key calculation shows $\mathrm{Im}(A \cdot z) = \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0$.

To show these are isometries, one can show that the group $\mathrm{SL}(2, \mathbb{R})$ is generated by matrices corresponding to elementary transformations known to be isometries:

1. Translations: $z \mapsto z + b$ for $b \in \mathbb{R}$, corresponding to $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.
2. Dilations: $z \mapsto \lambda z$ for $\lambda > 0$, corresponding to $\begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & 1/\sqrt{\lambda} \end{pmatrix}$.
3. Inversion: $z \mapsto -1/z$, corresponding to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

A direct calculation shows each of these generator types preserves the hyperbolic metric. Since any element of $\mathrm{SL}(2, \mathbb{R})$ can be expressed as a product of these elementary transformations (a consequence of row reduction), the entire group acts by isometries. □

Corollary 1.15. *Since elements of $\mathrm{SL}(2, \mathbb{R})$ are isometries, they map geodesics to geodesics. That is, if γ is a geodesic, then for any $A \in \mathrm{SL}(2, \mathbb{R})$, the curve $t \mapsto A \cdot \gamma(t)$ is also a geodesic.*

A fundamental property of the hyperbolic plane is its homogeneity and isotropy, captured by the following result.

Proposition 1.16. *The action of* $\mathrm{SL}(2,\mathbb{R})$ *on* $\mathbb{H}$ *is transitive. The stabilizer of the point* $i \in \mathbb{H}$ *is the special orthogonal group* $\mathrm{SO}(2)$*, the group of rotation matrices:*

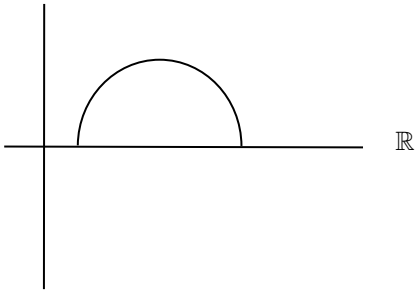
$$\mathrm{Stab}_{\mathrm{SL}(2,\mathbb{R})}(i) = \mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}.$$

Moreover, for any two points $z, z' \in \mathbb{H}$*, there exists an isometry* $A \in \mathrm{SL}(2,\mathbb{R})$ *that maps* z *to* i *and* z' *to a point on the positive imaginary axis,* yi*, for some* $y \geqslant 1$*.*

Corollary 1.17. *Any two distinct points in* $\mathbb{H}$ *are joined by a unique hyperbolic geodesic.*

Theorem 1.18. *The geodesics in* $\mathbb{H}$ *are precisely the Euclidean semicircles with centers on the real axis and the vertical rays perpendicular to the real axis.*

These curves are called generalized semicircles:



1.3 AM Problem Session

Problem 1.19. *Which of the groups* $\mathbb{Z}/2\mathbb{Z}$*,* $\mathbb{Z}/3\mathbb{Z}$*,* $\mathbb{Z}^2$ *admit a free action on* $\mathbb{R}$ *by isometries? What if* $\mathbb{R}$ *is replaced by* $\mathbb{R}\backslash\{0\}$*?*

Solution.

Group	On $\mathbb{R}$	On $\mathbb{R}\backslash\{0\}$
$\mathbb{Z}/2\mathbb{Z}$	No	Yes
$\mathbb{Z}/3\mathbb{Z}$	No	No
$\mathbb{Z}^2$	Yes	No

The isometries of $\mathbb{R}$ are translations $x \mapsto x + a$ and reflections $x \mapsto -x + a$, with $a \in \mathbb{R}$.

On $\mathbb{R}$:

- $\mathbb{Z}/2\mathbb{Z}$**:** Any nontrivial homomorphism must send the non-identity element to a reflection or the identity. Reflections fix a point, and the identity clearly does, so no free action exists.
- $\mathbb{Z}/3\mathbb{Z}$**:** Suppose a generator maps to a reflection. Then its square is the identity, so the image of k^2 is trivial, though $k^2 \neq \text{id}$. This contradicts freeness. A nontrivial element cannot map to a nontrivial translation since its order is finite but translations have infinite order. Hence, no free action exists.
- $\mathbb{Z}^2$**:** Suppose both generators map to translations: $x \mapsto x + a$, $x \mapsto x + b$. The action of $(m, n) \in \mathbb{Z}^2$ is then $x \mapsto x + ma + nb$. The action is free if and only if $ma + nb = 0$ implies $m = n = 0$, which holds if a and b are $\mathbb{Q}$-linearly independent. For example, $a = 1$, $b = \sqrt{2}$. So a free action exists.

On $\mathbb{R}\backslash\{0\}$:

- $\mathbb{Z}/2\mathbb{Z}$**:** Map the generator to $x \mapsto -x$. This fixes only $x = 0$, which is not in the domain, so the action is free.
- $\mathbb{Z}/3\mathbb{Z}$**:** Any homomorphism to $\mathbb{Z}/2\mathbb{Z}$ must be trivial, since 3 is not divisible by 2. The action is then trivial and not free.
- $\mathbb{Z}^2$**:** The image of any homomorphism lies in $\mathbb{Z}/2\mathbb{Z}$. If both generators map to $x \mapsto -x$, then their difference maps to the identity, hence acts trivially. So the action is not free.

□

Problem 1.20. *Show that any action of a finite group on a tree has a global fixed point.*

Solution. Let G be a finite group acting by isometries on a tree T. A point $p \in T$ (which may be a vertex or an interior point of an edge) is a global fixed point if $g \cdot p = p$ for all $g \in G$.

Our first step is to construct a finite, G-invariant subtree. Let v_0 be an arbitrary vertex of T. Consider its orbit under the action of G, $O(v_0) = \{g \cdot v_0 \mid g \in G\}$. Since G is finite, $O(v_0)$ is a finite set of vertices. In a tree, any finite set of vertices is contained in a unique minimal subtree, which can be identified as the convex hull of the set. Let Y be the convex hull of $O(v_0)$. Since $O(v_0)$ is finite, Y is a finite tree.

We now show that Y is invariant under the action of G. For any $g \in G$, the set $g \cdot Y$ is the convex hull of the set $g \cdot O(v_0)$. But since G is a group, $g \cdot O(v_0) = \{gh \cdot v_0 \mid h \in G\} = O(v_0)$. By the uniqueness of the minimal subtree containing a given set of vertices, we must have $g \cdot Y = Y$. Thus, the action of G on T restricts to an action on the finite tree Y.

The final step is to find a fixed point within Y. Every non-empty finite tree has a center, which consists of either a single vertex or a single edge (i.e., two adjacent vertices). The center is preserved by every automorphism of the tree. Since each $g \in G$ acts as a tree automorphism on Y, the center of Y, denoted $C(Y)$, must be invariant under the action of G. That is, for every $g \in G$, the map $p \mapsto g \cdot p$ sends $C(Y)$ to itself.

We consider two cases based on the structure of the center.

1. The center $C(Y)$ is a single vertex, v_c. Since $C(Y) = \{v_c\}$ is G-invariant, we must have $g \cdot v_c = v_c$ for all $g \in G$. Thus, v_c is a global fixed point.
2. The center $C(Y)$ is a single edge, e, connecting vertices v_1 and v_2. The set $\{v_1, v_2\}$ is invariant under G. This means for any $g \in G$, either g fixes both vertices ($g \cdot v_1 = v_1$ and $g \cdot v_2 = v_2$), or g swaps them ($g \cdot v_1 = v_2$ and $g \cdot v_2 = v_1$). If every $g \in G$ fixes both vertices, then v_1 is a global fixed point. If there exists some $h \in G$ that swaps them, consider the midpoint m of the edge e. An isometry that fixes the endpoints of a segment also fixes its midpoint. An isometry that swaps the endpoints of a segment also fixes its midpoint. Therefore, any $g \in G$, whether it fixes or swaps v_1 and v_2, must fix the point m. Thus, m is a global fixed point.

In every case, we have found a point in Y (and thus in T) that is fixed by every element of G.

□

Problem 1.21.

1. *Check that the curve $\gamma(t) = i\exp(t)$ is a geodesic in the hyperbolic plane $\mathbb{H}$.*
2. *Check that the map $z \mapsto -\frac{1}{z}$ is an isometry of the hyperbolic plane $\mathbb{H}$.*
3. *Verify that the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$ by Möbius transformations is indeed an action.*
4. *Complete the proof that if points $z, z', w, w' \in \mathbb{H}$ satisfy $d_{\mathbb{H}}(z, z') = d_{\mathbb{H}}(w, w')$, then there is a matrix $A \in \mathrm{SL}_2(\mathbb{R})$ such that $Az = w$ and $Az' = w'$. Is the matrix unique?*

Solution.

1. A curve $\gamma(t)$ is a geodesic if it is parameterized by arc length, meaning the hyperbolic length of the curve from $\gamma(s)$ to $\gamma(t)$ is $|t - s|$. For $\gamma(t) = ie^t$, its velocity vector is $\dot{\gamma}(t) = ie^t$ and its imaginary part is $\mathrm{im}(\gamma(t)) = e^t$. The hyperbolic speed is

$$||\dot{\gamma}(t)||_{\gamma(t)} = \frac{|\dot{\gamma}(t)|_{\mathbb{R}^2}}{\mathrm{im}(\gamma(t))} = \frac{|ie^t|}{e^t} = \frac{e^t}{e^t} = 1.$$

The length of the path from $t = s$ to $t = t_0 > s$ is $\int_s^{t_0} 1\,dt = t_0 - s$. Since the path length equals the change in the parameter, the curve is parameterized by arc length. As vertical lines are known to be the shortest paths in $\mathbb{H}$, this curve is a geodesic.

2. A holomorphic map $f : \mathbb{H} \to \mathbb{H}$ is a Riemannian isometry if it satisfies $|f'(z)|/\operatorname{im}(f(z)) = 1/\operatorname{im}(z)$. Let $f(z) = -1/z$. Its derivative is $f'(z) = 1/z^2$. The imaginary part is

$$\operatorname{im}(f(z)) = \operatorname{im}(-1/z) = \operatorname{im}(-\overline{z}/|z|^2) = \operatorname{im}(z)/|z|^2.$$

The condition becomes

$$\frac{|1/z^2|}{\operatorname{im}(z)/|z|^2} = \frac{1/|z|^2}{\operatorname{im}(z)/|z|^2} = \frac{1}{\operatorname{im}(z)}.$$

Since the condition holds, $f(z) = -1/z$ is an isometry.

3. The action of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ (so $ad - bc = 1$) on $z \in \mathbb{H}$ is $A \cdot z = \frac{az+b}{cz+d}$.

First, for closure, we must show $A \cdot z \in \mathbb{H}$. $\operatorname{im}(A \cdot z) = \operatorname{im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right)$. The imaginary part of the numerator is $(ad - bc)\operatorname{im}(z) = \operatorname{im}(z)$. So

$$\operatorname{im}(A \cdot z) = \frac{\operatorname{im}(z)}{|cz + d|^2} > 0,$$

as $\operatorname{im}(z) > 0$ and $cz + d \neq 0$ for $z \in \mathbb{H}, A \in \mathrm{SL}_2(\mathbb{R})$. Each such map is a bijection $\mathbb{H} \to \mathbb{H}$.

Second, the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ acts as $I \cdot z = \frac{1z+0}{0z+1} = z$.

Third, for compatibility, let $A, B \in \mathrm{SL}_2(\mathbb{R})$. Let $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$. Then

$$\begin{aligned}
(AB) \cdot z &= \frac{(a_1a_2 + b_1c_2)z + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)z + (c_1b_2 + d_1d_2)} \\
&= \frac{a_1\left(\frac{a_2z+b_2}{c_2z+d_2}\right) + b_1}{c_1\left(\frac{a_2z+b_2}{c_2z+d_2}\right) + d_1} = \frac{a_1(a_2z + b_2) + b_1(c_2z + d_2)}{c_1(a_2z + b_2) + d_1(c_2z + d_2)} \\
&= A \cdot \left(\frac{a_2z + b_2}{c_2z + d_2}\right) \\
&= A \cdot (B \cdot z).
\end{aligned}$$

Thus, this defines a valid group action.

4. Let $d_0 = d_{\mathbb{H}}(z, z') = d_{\mathbb{H}}(w, w')$. The transitivity of the $\mathrm{SL}_2(\mathbb{R})$ action allows us to simplify the problem. By Proposition 1.16, there exists an isometry $A_1 \in \mathrm{SL}_2(\mathbb{R})$ such that $A_1 z = i$ and $A_1 z' = ie^{d_0}$. Similarly, there exists $A_2 \in \mathrm{SL}_2(\mathbb{R})$ such that $A_2 w = i$ and $A_2 w' = ie^{d_0}$. Let $A = A_2^{-1} A_1$. Then $A \in \mathrm{SL}_2(\mathbb{R})$ and $Az = A_2^{-1}(A_1 z) = A_2^{-1}(i) = w$, and $Az' = A_2^{-1}(A_1 z') = A_2^{-1}(ie^{d_0}) = w'$. So such a matrix A exists.

   For uniqueness, suppose another matrix $B \in \mathrm{SL}_2(\mathbb{R})$ satisfies $Bz = w$ and $Bz' = w'$. Then the matrix $M = A^{-1}B$ satisfies $Mw = w$ and $Mw' = w'$. If $z \neq z'$, then $w \neq w'$. An orientation-preserving isometry of $\mathbb{H}$ that fixes two distinct points must be the identity map. The mapping from $\mathrm{SL}_2(\mathbb{R})$ to the group of isometries has kernel $\{\pm I\}$. Thus, M must be either I or $-I$. This implies $B = \pm A$. The matrix is unique up to sign. If $z = z'$, then $d_0 = 0$ and $w = w'$. The condition is simply $Az = w$. The set of such matrices is the coset $A_0 \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(z)$, where A_0 is any one such matrix. Since the stabilizer is the infinite group $\mathrm{SO}(2)$ (up to conjugacy), the matrix is not unique in this case.

□

Problem 1.22.

1. *Check that the function* $z \mapsto -\frac{1}{z} = -\frac{\bar{z}}{|z|^2}$ *maps generalized semicircles to generalized semicircles.*
2. *Check that the group* $\mathrm{SL}_2(\mathbb{R})$ *acts transitively on the set of generalized semicircles in* $\mathbb{H}$.

Solution.

1. A generalized circle in $\mathbb{C}$ is described by the equation $Kz\bar{z} + Lz + \bar{L}\bar{z} + M = 0$ for $K, M \in \mathbb{R}$ and $L \in \mathbb{C}$. For this circle to be orthogonal to the real axis $\mathbb{R}$, its center (if $K \neq 0$) must be on $\mathbb{R}$, or it must be a vertical line (if $K = 0$). Both conditions are met if and only if the coefficient L is a real number. The equation for such an orthogonal generalized circle thus simplifies to $Kz\bar{z} + L(z + \bar{z}) + M = 0$.

   Let $w = -1/z$, which implies $z = -1/w$. We substitute this into the equation for our orthogonal generalized circle:

$$\begin{aligned} & K\left(-\frac{1}{w}\right)\left(-\frac{1}{\bar{w}}\right) + L\left(-\frac{1}{w} - \frac{1}{\bar{w}}\right) + M = 0 \\ \implies & \frac{K}{w\bar{w}} - L\left(\frac{w + \bar{w}}{w\bar{w}}\right) + M = 0 \\ \implies & K - L(w + \bar{w}) + M(w\bar{w}) = 0 \\ \implies & M(w\bar{w}) - L(w + \bar{w}) + K = 0 \end{aligned}$$

This is the equation of a new generalized circle. Its coefficients are $K' = M$, $L' = -L$, and $M' = K$. Since L is real, $L' = -L$ is also real. Therefore, the resulting curve is also a generalized circle orthogonal to the real axis.

Finally, the map $z \mapsto -1/z$ preserves the upper half-plane $\mathbb{H}$, since $\mathrm{Im}(-1/z) = \mathrm{Im}(-\bar{z}/|z|^2) = \mathrm{Im}(z)/|z|^2 > 0$ if $\mathrm{Im}(z) > 0$. Thus, the image of a generalized semicircle in $\mathbb{H}$ is another generalized semicircle in $\mathbb{H}$.

2. Let $\mathcal{G}$ be the set of generalized semicircles in $\mathbb{H}$. To show the action of $\mathrm{SL}(2,\mathbb{R})$ on $\mathcal{G}$ is transitive, it suffices to show that any geodesic $C \in \mathcal{G}$ can be mapped to the positive imaginary axis, $L_0 = \{iy \mid y > 0\}$. A geodesic is determined by its endpoints on $\mathbb{R} \cup \{\infty\}$. The endpoints of L_0 are $\{0, \infty\}$. Let C have endpoints $\{p, q\}$.

   - Case 1: $p, q \in \mathbb{R}$. The transformation $f(z) = \frac{z-p}{z-q}$ maps $p \mapsto 0$ and $q \mapsto \infty$. The corresponding matrix $\begin{pmatrix} 1 & -p \\ 1 & -q \end{pmatrix}$ has determinant $p - q$. It can be scaled by $1/\sqrt{|p-q|}$ and its entries' signs adjusted to produce a matrix in $\mathrm{SL}(2,\mathbb{R})$ that achieves the same mapping of endpoints.
   - Case 2: $p \in \mathbb{R}, q = \infty$. The translation $f(z) = z - p$ maps $p \mapsto 0$ and $\infty \mapsto \infty$. This corresponds to the matrix $A = \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$.

   Since any geodesic can be mapped to L_0, for any $C_1, C_2 \in \mathcal{G}$, there exists an $A \in \mathrm{SL}(2,\mathbb{R})$ mapping C_1 to C_2. Thus, the action is transitive.

□

Problem 1.23. *Consider the function $I : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$ defined by $I(z) = \frac{z-i}{z+i}$.*

1. *Show that I restricts to a bijection from the upper half plane $\mathbb{H}$ to the open unit disk $\mathbb{D} = \{w \in \mathbb{C} : |w| < 1\}$.*
2. *Check that I takes the hyperbolic pointwise inner product on $\mathbb{H}$ to the pointwise inner product on $\mathbb{D}$ given by*

$$\langle \alpha, \beta \rangle_w^{\mathbb{D}} = \frac{4}{(1-|w|^2)^2} \langle \alpha, \beta \rangle_{\mathbb{R}^2}.$$

3. *Check that I takes generalized semicircles in $\mathbb{H}$ to generalized diameters in $\mathbb{D}$.*

Solution.

1. Let $z = x + iy \in \mathbb{H}$, so $y > 0$. We compute

$$\begin{aligned} |I(z)|^2 &= \left|\frac{z-i}{z+i}\right|^2 \\ &= \frac{|x+i(y-1)|^2}{|x+i(y+1)|^2} \\ &= \frac{x^2+(y-1)^2}{x^2+(y+1)^2}. \end{aligned}$$

Since $y > 0$, we have $0 \leqslant (y-1)^2 < (y+1)^2$, which implies $|I(z)|^2 < 1$. Thus, $I(\mathbb{H}) \subseteq \mathbb{D}$.

To show it is a bijection, we find the inverse. Solving $w = \frac{z-i}{z+i}$ for z yields $z = i\frac{1+w}{1-w}$. Let $w \in \mathbb{D}$. We must show $z \in \mathbb{H}$. We compute

$$\begin{aligned} \operatorname{im}(z) &= \operatorname{im}\left(i\frac{1+w}{1-w}\right) \\ &= \operatorname{Re}\left(\frac{1+w}{1-w}\right) \\ &= \operatorname{Re}\left(\frac{(1+w)(1-\bar{w})}{|1-w|^2}\right) \\ &= \frac{\operatorname{Re}(1+w-\bar{w}-|w|^2)}{|1-w|^2} \\ &= \frac{1-|w|^2}{|1-w|^2}. \end{aligned}$$

Since $|w| < 1$ for $w \in \mathbb{D}$, $1 - |w|^2 > 0$, so $\operatorname{im}(z) > 0$. Thus, $I^{-1}(\mathbb{D}) \subseteq \mathbb{H}$. The existence of a well-defined inverse mapping between the domains confirms I is a bijection.

2. The map I is an isometry if it pulls back the disk metric to the half-plane metric. For a holomorphic map, this requires satisfying the condition

$$\frac{1}{(\operatorname{im} z)^2} = \frac{4|I'(z)|^2}{(1-|I(z)|^2)^2}.$$

First, we compute the components. The derivative is $I'(z) = \frac{(z+i)-(z-i)}{(z+i)^2} = \frac{2i}{(z+i)^2}$. Thus, $|I'(z)|^2 = \frac{4}{|z+i|^4}$. From the previous part, we have the identity $1 - |I(z)|^2 = \frac{4\operatorname{im}(z)}{|z+i|^2}$. Substituting these into the right-hand side of the condition gives:

$$\frac{4\left(\frac{4}{|z+i|^4}\right)}{\left(\frac{4\operatorname{im}(z)}{|z+i|^2}\right)^2} = \frac{16/|z+i|^4}{16(\operatorname{im} z)^2/|z+i|^4} = \frac{1}{(\operatorname{im} z)^2}.$$

The condition holds, so I is a Riemannian isometry, and therefore a metric isometry.

3. This follows directly from the fact that I is an isometry. Isometries map geodesics to geodesics. The geodesics of $\mathbb{H}$ are the generalized semicircles. The geodesics of the Poincaré disk $\mathbb{D}$ are the generalized diameters (Euclidean diameters and circular arcs orthogonal to the boundary circle $\partial\mathbb{D}$). Therefore, I must map generalized semicircles in $\mathbb{H}$ to generalized diameters in $\mathbb{D}$.

   Alternatively, one can use a geometric argument: I is a Möbius transformation that maps the boundary of $\mathbb{H}$ (the real axis) to the boundary of $\mathbb{D}$ (the unit circle). Since I is conformal, it maps curves orthogonal to the real axis to curves orthogonal to the unit circle, which is precisely the characterization of geodesics in each model.

□

Problem 1.24. *The hyperbolic area of a region $A \subset \mathbb{H}$ is $\iint_A \frac{1}{y^2}\,dx\,dy$.*

1. *Compute the area of the hyperbolic region bounded by an arc of the unit circle and two upward-pointing vertical rays, one meeting the circle at angle θ and the other at angle ϕ. (This is a triangle with angles $\theta, \phi, 0$).*
2. *Compute the area of a hyperbolic triangle with angles α, β, γ bounded by an arc of the unit circle, a vertical segment, and another circular arc.*
3. *Use the fact that isometries preserve angles and area to prove that the area of any triangle with angles α, β, γ is $\pi - (\alpha + \beta + \gamma)$.*
4. *For $r > 0$, consider $B_r(i) = \{z \in \mathbb{H} | d_{\mathbb{H}}(i, z) < r\}$. For $r > 10$, show Area($B_r(i)$) is exponential in r. Hint: Show $B_r(i)$ contains $Q_r = \{x + iy | 0 \leqslant x \leqslant e^{r/10}, 1 \leqslant y \leqslant e^{r/2}\}$ and calculate its area.*
5. *Use previous results to show hyperbolic triangles are slim.*

Solution.

1. This region is a hyperbolic triangle with one ideal vertex at $i\infty$ (where the two vertical rays meet, with an interior angle of 0) and two finite vertices on the unit circle in $\mathbb{H}$. Let the two finite vertices be V_1 and V_2. The sides are segments of two vertical lines and an arc of the unit circle $x^2 + y^2 = 1$.

   The angle between two intersecting geodesics is the Euclidean angle between their tangent vectors at the intersection point. Let the rightmost vertex be $V_1 = (x_1, y_1)$ where the vertical line $x = x_1$ meets the unit circle. The interior angle is ϕ. The tangent to the vertical line is a vertical vector. The tangent to the unit circle is perpendicular to the radial vector from the origin $(0, 0)$ to V_1. The angle ϕ is the angle between the vertical tangent and the circle's tangent. By geometry, this is equal to the angle the radial vector makes with the horizontal axis. Thus, $\cos(\phi) = x_1$. Similarly, for the left vertex $V_2 = (x_2, y_2)$ with interior angle θ, we have $x_2 = -\cos(\theta)$ (assuming the vertices are on opposite sides of the imaginary axis).

The region is described by $\{(x, y) \in \mathbb{H} \mid -\cos\theta \leqslant x \leqslant \cos\phi,\ y \geqslant \sqrt{1-x^2}\}$. The hyperbolic area is given by the integral:

$$\text{Area} = \int_{-\cos\theta}^{\cos\phi} \left(\int_{\sqrt{1-x^2}}^{\infty} \frac{1}{y^2}\, dy \right) dx$$

The inner integral evaluates to:

$$\int_{\sqrt{1-x^2}}^{\infty} y^{-2}\, dy = \left[-\frac{1}{y} \right]_{\sqrt{1-x^2}}^{\infty} = 0 - \left(-\frac{1}{\sqrt{1-x^2}} \right) = \frac{1}{\sqrt{1-x^2}}$$

Now we compute the outer integral:

$$\text{Area} = \int_{-\cos\theta}^{\cos\phi} \frac{1}{\sqrt{1-x^2}}\, dx = [\arcsin(x)]_{-\cos\theta}^{\cos\phi}$$

$$= \arcsin(\cos\phi) - \arcsin(-\cos\theta) = \arcsin(\cos\phi) + \arcsin(\cos\theta)$$

Using the identity $\arcsin(\cos(z)) = \pi/2 - z$ for $z \in [0, \pi]$, we get:

$$\text{Area} = \left(\frac{\pi}{2} - \phi \right) + \left(\frac{\pi}{2} - \theta \right) = \pi - \theta - \phi.$$

This establishes the area formula for any singly-ideal triangle (a triangle with one ideal vertex).

2. We solve parts 2 and 3 together. We will now compute the area of a general hyperbolic triangle with angles α, β, γ by using the result from part (1) and a geometric decomposition. The result is that the area is its angle deficit: $\pi - (\alpha + \beta + \gamma)$.

   Let T be a triangle with vertices A, B, C and corresponding interior angles α, β, γ. The strategy is to express the area of T in terms of singly-ideal triangles, whose areas we can calculate using the formula from part (1). Extend the geodesic side BC to one of its ideal endpoints on the boundary of $\mathbb{H}$, let's call this ideal point P. We can choose P such that the vertex C lies on the geodesic segment between B and P. Now, draw the geodesic from vertex A to the ideal point P. This construction creates two new singly-ideal triangles, T_{ABP} and T_{ACP}, which share the side AP. The original triangle T_{ABC} can be seen as the difference in area of these two singly-ideal triangles:

   $$\text{Area}(T_{ABC}) = \text{Area}(T_{ABP}) - \text{Area}(T_{ACP}).$$

   Now we analyze the angles of these singly-ideal triangles to compute their areas using the formula $\text{Area}(v_1, v_2, 0) = \pi - v_1 - v_2$.

   - Triangle T_{ABP}: The vertices are A, B, P. The angle at the ideal vertex P is 0. The angle at vertex B is the same as in the original triangle, so it is β. The angle at vertex A is the entire angle $\angle BAP$. So, its area is:

     $$\text{Area}(T_{ABP}) = \pi - \beta - \angle BAP.$$

- Triangle T_{ACP}: The vertices are A, C, P. The angle at the ideal vertex P is 0. The angle at vertex C is supplementary to γ, since it is an exterior angle on the straight geodesic through B, C, P. So, the interior angle of T_{ACP} at C is $\pi - \gamma$. The angle at vertex A is $\angle CAP$. So, its area is:

$$\text{Area}(T_{ACP}) = \pi - (\pi - \gamma) - \angle CAP = \gamma - \angle CAP.$$

The angle α of the original triangle at vertex A is the difference between the angles of the larger and smaller triangles at that vertex:

$$\alpha = \angle BAC = \angle BAP - \angle CAP.$$

From this, we can express $\angle BAP$ as $\angle BAP = \alpha + \angle CAP$.

Now, substitute these expressions back into the area difference formula:

$$\text{Area}(T_{ABC}) = (\pi - \beta - \angle BAP) - (\gamma - \angle CAP)$$

$$= \pi - \beta - (\alpha + \angle CAP) - \gamma + \angle CAP$$

The $\angle CAP$ terms cancel out, leaving:

$$\text{Area}(T_{ABC}) = \pi - \alpha - \beta - \gamma.$$

This proves that the area of any hyperbolic triangle is its angle deficit.

3. The distance from i to $z = x + iy$ is $d_{\mathbb{H}}(i, z) = \text{arccosh}\left(\frac{x^2+y^2+1}{2y}\right)$. We want to show $Q_r = \{x + iy \mid 0 \leqslant x \leqslant e^{r/10}, 1 \leqslant y \leqslant e^{r/2}\} \subset B_r(i)$ for $r > 10$. This requires $d_{\mathbb{H}}(i, z) < r$ for all $z \in Q_r$, which is equivalent to $\frac{x^2+y^2+1}{2y} < \cosh(r)$. Let $f(x, y) = \frac{x^2+y^2+1}{2y}$. We must find the maximum of f on the compact set Q_r. The maximum must occur on the boundary of Q_r.

   - On $y = 1$: $f(x, 1) = (x^2+2)/2$. Max at $x = e^{r/10}$, value is $(e^{r/5}+2)/2$.
   - On $x = e^{r/10}$: $f(e^{r/10}, y) = \frac{e^{r/5}+y^2+1}{2y} = \frac{e^{r/5}+1}{2y} + \frac{y}{2}$. This function of y is minimized when $y^2 = e^{r/5} + 1$ and increases away from this minimum. We check the endpoints $y = 1$ and $y = e^{r/2}$. We already have the value at $y = 1$. At $y = e^{r/2}$, the value is $\frac{e^{r/5}+e^r+1}{2e^{r/2}} = \frac{1}{2}(e^{-3r/10} + e^{r/2} + e^{-r/2})$.

   For large r (specifically $r > 10$), the dominant term is $\frac{1}{2}e^{r/2}$. We need to check if $\frac{1}{2}e^{r/2} < \cosh(r) = \frac{e^r+e^{-r}}{2}$. This is equivalent to $e^{r/2} < e^r + e^{-r}$, which is clearly true for $r > 0$. Thus, $Q_r \subset B_r(i)$.

   The area of Q_r is:

$$\text{Area}(Q_r) = \int_0^{e^{r/10}} \int_1^{e^{r/2}} \frac{1}{y^2}\, dy\, dx = \int_0^{e^{r/10}} \left[-\frac{1}{y}\right]_1^{e^{r/2}} dx$$

$$= \int_0^{e^{r/10}} (1 - e^{-r/2})\, dx = (1 - e^{-r/2})e^{r/10} = e^{r/10} - e^{-2r/5}$$

Since $B_r(i)$ contains Q_r, its area is bounded below: $\text{Area}(B_r(i)) \geqslant e^{r/10} - e^{-2r/5}$. For large r, this grows like $e^{0.1r}$, which is exponential in r.

4. A geodesic space is δ-slim if for any geodesic triangle, every point on one side is within a distance δ of the union of the other two sides. We must show there is a universal $\delta > 0$ for all triangles in $\mathbb{H}$.

   Assume, for the sake of contradiction, that hyperbolic triangles are not slim. This means that for any candidate constant $\delta > 0$, we can find a geodesic triangle T and a point p on one of its sides such that the hyperbolic distance from p to the union of the other two sides is greater than δ.

   This implies that the open hyperbolic ball $B(p, \delta)$ centered at p with radius δ is contained entirely within the triangle T. Therefore, the area of the ball must be less than or equal to the area of the triangle:

   $$\text{Area}(B(p, \delta)) \leqslant \text{Area}(T).$$

   From part (3), we know the area of any hyperbolic triangle is bounded above by π: $\text{Area}(T) = \pi - (\alpha + \beta + \gamma) < \pi$. From part (4), we know that the area of a hyperbolic ball of radius δ grows exponentially. Since area is isometry-invariant, $\text{Area}(B(p, \delta)) = \text{Area}(B(i, \delta))$. For large δ, this area is bounded below by a function of the form $Ke^{c\delta}$ for some positive constants K, c.

   So, for any $\delta > 0$, our assumption implies we can find a triangle such that:

   $$Ke^{c\delta} \leqslant \text{Area}(B(p, \delta)) \leqslant \text{Area}(T) < \pi.$$

   However, the term $Ke^{c\delta}$ grows without bound as $\delta \to \infty$. We can always choose a δ large enough such that $Ke^{c\delta} > \pi$. This is a contradiction.

   Therefore, our initial assumption must be false. There must exist a universal upper bound δ on the radius of any ball that can be inscribed in a triangle in this manner. This proves that hyperbolic triangles are slim.

□

1.4 PM Session 1: Introduction to Riemann Surfaces

The big goal of this week is to understand why certain numbers, like

$$e^{\pi\sqrt{163}} \approx 262537412640768743.99999925...$$

are extraordinarily close to integers. This phenomenon is connected to the theory of complex multiplication, elliptic curves, and modular forms, so we need to introduce some notions of complex analysis on Riemann surfaces.

Our journey in analysis often starts with understanding the number systems we work with, each extending the capabilities of the previous one:

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}.$$

- **Integers ($\mathbb{Z}$):** The set $\{\dots, -2, -1, 0, 1, 2, \dots\}$. $\mathbb{Z}$ is not closed under division. For example, $2x - 1 = 0$ has no solution in $\mathbb{Z}$.
- **Rational Numbers ($\mathbb{Q}$):** To solve linear equations of the form $\alpha x + \beta = 0$ (where $\alpha, \beta \in \mathbb{Z}, \alpha \neq 0$), we extend to the field of rational numbers, $\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\right\}$. $\mathbb{Q}$ is an algebraic field, meaning it's closed under basic arithmetic operations.
- **Real Numbers ($\mathbb{R}$):** The field $\mathbb{Q}$ is still "incomplete" in an analytic sense; it has "holes." For instance, the sequence $1, 1.4, 1.41, 1.414, \dots$ (approximating $\sqrt{2}$) consists of rational numbers, but its limit, $\sqrt{2}$, is not rational. $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual metric, meaning every Cauchy sequence of real numbers converges to a real number. This completeness is important for calculus (limits, continuity, derivatives, integrals).
- **Complex Numbers ($\mathbb{C}$):** Even $\mathbb{R}$ is not algebraically complete. The equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$. We introduce the imaginary unit i such that $i^2 = -1$ and define the field of complex numbers as $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$. The arithmetic operations are defined as:
  - Addition: $(a + ib) + (c + id) = (a + c) + i(b + d)$
  - Multiplication: $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$

  By the Fundamental Theorem of Algebra, every non-constant single-variable polynomial with complex coefficients has at least one complex root, so $\mathbb{C}$ is algebraically closed.

Our goal is to develop analysis over $\mathbb{C}$ in a way analogous to how it's done over $\mathbb{R}$.

Definition 1.25. *Let $U \subseteq \mathbb{C}$ be an open set. A function $f : U \to \mathbb{C}$ is said to be $\mathbb{C}$-**differentiable** (or **holomorphic**, or **analytic**) at a point $z_0 \in U$ if the limit*

$$f'(z_0) = \lim_{h \to 0} \frac{f(z_0 + h) - f(z_0)}{h}$$

exists. If f is $\mathbb{C}$-differentiable at every point in U, we say f is holomorphic on U.

Note that h approaches 0 in the complex plane, meaning it can approach from any direction. This is a much stronger condition than real differentiability.

Proposition 1.26. *If a function $f : U \to \mathbb{C}$ is holomorphic on an open set U, then f is infinitely differentiable on U. Moreover, for any $z_0 \in U$, f can be*

represented by a convergent power series in a neighborhood of z_0: there exists an open disc $D(z_0, r) \subseteq U$ (for some $r > 0$) such that

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

for all $z \in D(z_0, r)$. The coefficients are given by $a_n = \frac{f^{(n)}(z_0)}{n!}$.

This property (being locally representable by a power series) is why holomorphic functions are also called analytic functions.

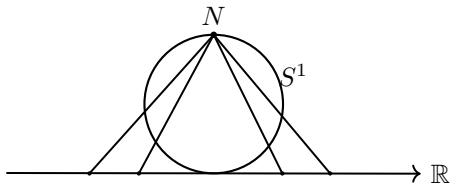
Exercise 1.27. *Show that this proposition is false over $\mathbb{R}$. That is, find a function $f : \mathbb{R} \to \mathbb{R}$ that is infinitely $\mathbb{R}$-differentiable but not equal to its Taylor series in any neighborhood of some point.*

Proof. See the problem session. □

Just as real analysis on $\mathbb{R}$ and $\mathbb{R}^n$ generalizes to analysis on real manifolds (spaces that locally look like Euclidean space), complex analysis on $\mathbb{C}$ generalizes to analysis on complex manifolds.

Example 1.28 (Real Manifolds)**.**

- *The circle $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. Using stereographic projection from the North pole $N = (0, 1)$, $S^1 \backslash \{N\}$ is homeomorphic to $\mathbb{R}$. Similarly, $S^1 \backslash \{S\}$ (where $S = (0, -1)$ is the South pole) is homeomorphic to $\mathbb{R}$. These homeomorphisms provide local coordinate charts.*



- *The sphere $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$. Stereographic projection from $S^2 \backslash \{N\}$ gives a homeomorphism to $\mathbb{R}^2 \cong \mathbb{C}$. This is an important example as it can be given a Riemann surface structure (the Riemann sphere).*
- *The torus $S^1 \times S^1$. We can cover it with charts, for example, by taking products of charts for S^1. E.g., $(S^1 \backslash \{N_1\}) \times (S^1 \backslash \{N_2\}) \cong \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.*

Definition 1.29. *Let X be a connected Hausdorff topological space. We say X is a **Riemann surface** if:*

- *There exists a cover $\{U_\alpha\}$ of X such that for each α, U_α is homeomorphic to an open subset V_α of $\mathbb{C}$ via a map ϕ_α:*

$$U_\alpha \xrightarrow{\sim \phi_\alpha} V_\alpha \overset{open}{\hookrightarrow} \mathbb{R}^2 \cong \mathbb{C}.$$

- *If two such charts (U_α, ϕ_α) and (U_β, ϕ_β) overlap, the transition map $\phi_\beta \circ \phi_\alpha^{-1}$ (from $\phi_\alpha(U_\alpha \cap U_\beta)$ to $\phi_\beta(U_\alpha \cap U_\beta)$) must be a holomorphic function between open sets in $\mathbb{C}$*

Remark 1.30. *The second condition is so that we have a consistent notion of complex analysis across X. This condition that transition maps are holomorphic is what makes it a complex manifold of dimension one (a Riemann surface), rather than just a 2-dimensional real manifold.*

Example 1.31.

1. *$\mathbb{C}$ itself is a Riemann surface. We can use a single chart $(U_1 = \mathbb{C}, \phi_1(z) = z)$. The transition map condition is trivially satisfied.*
2. *Any open subset $U \subseteq \mathbb{C}$ is a Riemann surface with the chart (U, id_U).*
3. *The **unit disc** $\Delta = \{z \in \mathbb{C} \mid |z| < 1\}$ is a Riemann surface.*
4. *The **upper half-plane** $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$ is a Riemann surface. This will be important for constructing modular forms.*

Remark 1.32. *Topologically, Δ is homeomorphic to $\mathbb{C}$ (and to $\mathbb{R}^2$). For example, $z \mapsto \frac{z}{1-|z|}$ is a homeomorphism from Δ to $\mathbb{C}$. However, as Riemann surfaces, they are very different. For example, $\mathbb{C}$ is not biholomorphic to Δ.*

Definition 1.33. *Let X be a Riemann surface with atlas $\{(U_\alpha, \phi_\alpha)\}$. A function $f : X \to \mathbb{C}$ is **holomorphic** at $p \in X$ if for any chart (U_α, ϕ_α) such that $p \in U_\alpha$, the composition $f \circ \phi_\alpha^{-1} : \phi_\alpha(U_\alpha) \to \mathbb{C}$ is holomorphic (in the usual sense for functions on open subsets of $\mathbb{C}$) at $\phi_\alpha(p)$. If f is holomorphic at every $p \in X$, then f is holomorphic on X.*

Definition 1.34. *A function $f : X \to \mathbb{C}$ is **holomorphic** if $f|_{U_\alpha}$ is holomorphic for all α.*

Definition 1.35. *A map of Riemann surfaces $\varphi : X \to Y$ is **holomorphic** if it satisfies the following conditions:*

- *φ is continuous;*
- *for every open set $V_\beta \subseteq Y$ and every holomorphic function $f : V_\beta \to \mathbb{C}$, the composition*
$$f \circ \varphi : \varphi^{-1}(V_\beta) \to \mathbb{C}$$
is holomorphic on $\varphi^{-1}(V_\beta) \subseteq X$.

The situation can be visualized in the following commutative diagram:

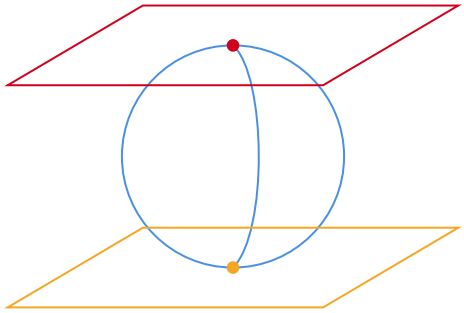
$$\begin{array}{ccccc} X & \xrightarrow{\varphi} & Y & & \\ \cup & & \cup & & \\ \varphi^{-1}(V_\beta) & \xrightarrow{\varphi} & V_\beta & \xrightarrow{f} & \mathbb{C} \end{array}$$

Proposition 1.36. *There exists no non-constant holomorphic map $\varphi : \mathbb{C} \to \Delta$.*

Proof. If $\varphi : \mathbb{C} \to \Delta$ were such a map, it would be an entire function (holomorphic on all of $\mathbb{C}$) whose image is contained in the unit disc Δ. Thus, $|\varphi(z)| < 1$ for all $z \in \mathbb{C}$, meaning φ is a bounded entire function. By Liouville's Theorem, any bounded entire function must be constant. □

1.5 PM Session 2: Introduction to Riemann Surfaces II

Example 1.37. *Consider $S^2 = (S^2 \backslash \{N\}) \cup (S^2 \backslash \{S\})$. By stereographic projection, $S^2 \backslash \{N\} \simeq \mathbb{R}^2 \simeq S^2 \backslash \{S\}$.*



where points (x, y, z) on S^2 satisfy $x^2 + y^2 + z^2 = 1$.

This is the first nontrivial example of a Riemann surface. We have (S^2, complex structure) = $\mathbb{P}^1_{\mathbb{C}}$.

Proposition 1.38. *Let $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{C}$ be a holomorphic map. Then f is constant.*

Proof. Since f is holomorphic on $\mathbb{P}^1_{\mathbb{C}}$, it is bounded (as $\mathbb{P}^1_{\mathbb{C}}$ is compact and f is continuous, so $|f|$ attains its maximum). If we view f as a map from $\mathbb{C} \cup \{\infty\}$ to $\mathbb{C}$, its restriction to $\mathbb{C}$ is an entire function. Since f is bounded on $\mathbb{P}^1_{\mathbb{C}}$, it is bounded on $\mathbb{C}$. By Liouville's theorem, a bounded entire function is constant. Thus, f is constant on $\mathbb{C}$, and by continuity, it is constant on $\mathbb{P}^1_{\mathbb{C}}$. □

Example 1.39. *The upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\} = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}$ is an open subset of $\mathbb{R}^2 \cong \mathbb{C}$, and thus inherits a complex structure from $\mathbb{C}$.*

Theorem 1.40.

1. *$\mathbb{H}$ is biholomorphic to Δ (the open unit disk), for instance, via the transformation $z \mapsto \frac{z-i}{z+i}$. Also, Δ is not biholomorphic to $\mathbb{C}$.*
2. *S^2 (equivalently $\mathbb{P}^1_{\mathbb{C}}$) has a unique complex structure up to biholomorphism.*

The second part is quite difficult.

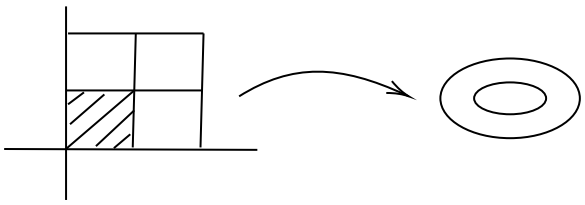
Example 1.41. *What about the torus $T^2 \cong S^1 \times S^1$? We have $S^1 \times S^1 \xrightarrow{\sim} (\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$. This can be identified with $\mathbb{C}/\Lambda_0$ where $\Lambda_0 = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot i$ is the lattice of Gaussian integers. The map from $(\mathbb{R}/\mathbb{Z}) \times (\mathbb{R}/\mathbb{Z})$ to $S^1 \times S^1$ is*

$([x],[y]) \mapsto (e^{2\pi ix}, e^{2\pi iy})$. *The map from* $\mathbb{C}$ *to* T^2 *for the lattice* Λ_0 *can be seen as* $z \mapsto (e^{2\pi iRe(z)}, e^{2\pi iIm(z)})$.

Definition 1.42. *A* ***lattice*** $\Lambda \subseteq \mathbb{C}$ *is a discrete subgroup of* $(\mathbb{C}, +)$ *isomorphic to* $\mathbb{Z}^2$. *Equivalently,* $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\}$ *for some* $\omega_1, \omega_2 \in \mathbb{C}$ *that are linearly independent over* $\mathbb{R}$ *(i.e.,* $\{\omega_1, \omega_2\}$ *forms an* $\mathbb{R}$*-basis for* $\mathbb{C}$*).*

Proposition 1.43. *For any lattice* $\Lambda \subset \mathbb{C}$*, the quotient space* $\mathbb{C}/\Lambda$ *is a Riemann surface.*

Proof. The projection map $\Pi : \mathbb{C} \to \mathbb{C}/\Lambda$ is a surjective local homeomorphism. For any point $z_0 \in \mathbb{C}$, there exists an open neighborhood $U \ni z_0$ such that $\Pi|_U : U \to \Pi(U)$ is a homeomorphism. Since $\mathbb{C}$ has a complex structure (given by the identity chart $z \mapsto z$), we can use Π to induce a complex structure on $\mathbb{C}/\Lambda$. Specifically, for any $[w] \in \mathbb{C}/\Lambda$, choose $z \in \mathbb{C}$ such that $\Pi(z) = [w]$. Let U_z be a neighborhood of z such that $\Pi|_{U_z}$ is injective. Then $(\Pi(U_z), (\Pi|_{U_z})^{-1})$ can serve as a chart around $[w]$. The transition maps between such charts are holomorphic because they are locally restrictions of translations in $\mathbb{C}$ (composed with identity maps), which are holomorphic.



The diagram illustrates a fundamental domain for $\mathbb{C}/\Lambda$ (a parallelogram) and its identification under Π.

$$\mathbb{C} \xrightarrow{\Pi} \mathbb{C}/\Lambda.$$

□

Problem 1.44. *Is there a unique complex structure on* $S^1 \times S^1$ *(topologically a torus)? Equivalently, is* $\mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda'$ *as Riemann surfaces for any two lattices* Λ *and* Λ'*?*

The answer is no, as we will see.

Proposition 1.45. *Let* $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ *be a holomorphic map of Riemann surfaces. Then:*

1. *There exists a holomorphic map $\tilde{\varphi} : \mathbb{C} \to \mathbb{C}$ such that the following diagram commutes (i.e., $\varphi \circ \pi = \pi' \circ \tilde{\varphi}$):*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\varphi}} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathbb{C}/\Lambda & \xrightarrow{\varphi} & \mathbb{C}/\Lambda' \end{array}$$

   This $\tilde{\varphi}$ is called a lift of φ.

2. *Any such lift $\tilde{\varphi}(z)$ must be an affine linear map, i.e., $\tilde{\varphi}(z) = \alpha z + \beta$ for some $\alpha, \beta \in \mathbb{C}$.*

Corollary 1.46. *Let $\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be a holomorphic map. If $\varphi([0]) = [0]$ (i.e., φ maps the origin of the first torus to the origin of the second), then φ is induced by a linear map $z \mapsto \alpha z$ for some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda'$.*

Corollary 1.47. *Two tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are biholomorphic, denoted $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}/\Lambda'$, if and only if there exists an $\alpha \in \mathbb{C}\backslash\{0\}$ such that $\alpha\Lambda = \Lambda'$.*

Note that this corollary implies that the distinct complex structures on $S^1 \times S^1$ (a topological torus) correspond to equivalence classes of lattices $\Lambda \subseteq \mathbb{C}$ under the equivalence relation $\Lambda \sim \Lambda'$ if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}\backslash\{0\}$ (i.e., lattices are equivalent if they are homothetic).

Consider two distinct lattices:

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$
$$\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$$

Since $\{\omega_1, \omega_2\}$ and $\{\omega_1', \omega_2'\}$ are $\mathbb{R}$-bases of $\mathbb{C}$ (when viewed as $\mathbb{R}^2$), there exists an invertible real 2×2 matrix $A \in \mathrm{GL}(2, \mathbb{R})$ that transforms one basis to the other.

The group of $\mathbb{R}$-linear automorphisms of $\mathbb{C}$ that are also $\mathbb{C}$-linear (i.e., multiplication by a non-zero complex number) can be identified with $\mathbb{C}^\times$. This embeds into $\mathrm{GL}(2, \mathbb{R})$ via the map $a + ib \mapsto \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. We have $\mathbb{C}$ acting on $\mathbb{C}$ by multiplication, and $\mathrm{GL}(2, \mathbb{R})$ acting on $\mathbb{R}^2$ by matrix multiplication. We identify $\mathbb{C}$ with $\mathbb{R}^2$. The set $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of $\mathbb{C}^\times$.

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{R}) & \longleftarrow & S^1 \\ \big\uparrow & & \cap \\ \mathrm{GL}_2(\mathbb{R}) & \longleftarrow & \mathbb{C}^\times \end{array}$$

The image of S^1 under the embedding $\mathbb{C}^\times \hookrightarrow \mathrm{GL}(2, \mathbb{R})$ is precisely $\mathrm{SO}(2, \mathbb{R})$ (the group of rotation matrices), which is a subgroup of $\mathrm{SL}(2, \mathbb{R})$.

The space of lattices, up to scaling by $\mathbb{C}^\times$ (homothety) and rotation (which can be absorbed into the scaling), can be parameterized. By scaling, any lattice Λ can be written as $c(\mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\tau)$ for some $c \in \mathbb{C}^\times$ and $\tau \in \mathbb{H}$ (the upper half-plane). The shape of the lattice is determined by τ. The space $\mathrm{SL}(2,\mathbb{R})/\mathrm{SO}(2,\mathbb{R})$ is isomorphic to $\mathbb{H}$. Thus, $\mathbb{H}$ serves as a parameter space for these normalized lattices. Remarkably, $\mathbb{H}$ is itself a Riemann surface, and it becomes the moduli space for complex structures on a torus once we further quotient by the action of $\mathrm{SL}(2,\mathbb{Z})$.

1.6 PM Problem Session

Problem 1.48. *Give an example of an infinitely differentiable $\mathbb{R}$-valued function which is not a power series.*

Solution. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} e^{-1/x^2} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

We show that f is smooth on $\mathbb{R}$ but not equal to its Taylor series at $x = 0$ in any neighborhood.

For $x \neq 0$, $f(x) = e^{-1/x^2}$ is a composition of smooth functions and thus smooth. By induction, its n-th derivative can be written as

$$f^{(n)}(x) = P_n(1/x)e^{-1/x^2},$$

where P_n is a polynomial. The base case is trivial. For the inductive step, assume the form holds for $n = k$. Differentiating yields

$$\begin{aligned} f^{(k+1)}(x) &= \frac{d}{dx}\left(P_k(1/x)e^{-1/x^2}\right) \\ &= \left(-\frac{1}{x^2}P_k'(1/x) + \frac{2}{x^3}P_k(1/x)\right)e^{-1/x^2} \\ &= P_{k+1}(1/x)e^{-1/x^2}, \end{aligned}$$

where $P_{k+1}(y) = -y^2P_k'(y) + 2y^3P_k(y)$, again a polynomial.

Now, we show that $f^{(n)}(0) = 0$ for all $n \geqslant 0$. Clearly, $f(0) = 0$. For $f'(0)$,

$$f'(0) = \lim_{h\to 0}\frac{f(h)}{h} = \lim_{h\to 0}\frac{e^{-1/h^2}}{h}.$$

Letting $y = 1/h$, this becomes $\lim_{|y|\to\infty}\frac{y}{e^{y^2}} = 0$, since the exponential dominates any polynomial. Similarly, assuming $f^{(k)}(0) = 0$, we find

$$f^{(k+1)}(0) = \lim_{h\to 0}\frac{f^{(k)}(h)}{h} = \lim_{h\to 0}\frac{P_k(1/h)e^{-1/h^2}}{h}.$$

With $y = 1/h$, this becomes $\lim_{|y|\to\infty} Q_k(y)e^{-y^2}$ for a polynomial $Q_k(y)$, which again tends to 0. Hence, all derivatives at 0 vanish.

The Taylor series of f at 0 is therefore

$$T(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n = 0,$$

yet $f(x) > 0$ for $x \neq 0$. Thus, f is smooth but not equal to its Taylor series in any neighborhood of 0.

□

Problem 1.49. *Write down the standard Riemann surface structure on S^2.*

Solution. The standard Riemann surface structure on the 2-sphere $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ identifies it with the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$. This structure is defined by an atlas of two charts given by stereographic projections from the North and South poles.

Let $N = (0, 0, 1)$ and $S = (0, 0, -1)$. Define:

- $U_1 = S^2\backslash\{N\}$ with chart map $\phi_1 : U_1 \to \mathbb{C}$ via stereographic projection from N:

$$\phi_1(x, y, z) = \frac{x + iy}{1 - z}, \quad \phi_1^{-1}(p) = \left(\frac{2\Re(p)}{1 + |w|^2}, \frac{2\Im(p)}{1 + |w|^2}, \frac{|w|^2 - 1}{|w|^2 + 1}\right)$$

- $U_2 = S^2\backslash\{S\}$ with chart map $\phi_2 : U_2 \to \mathbb{C}$ via stereographic projection from S:

$$\phi_2(x, y, z) = \frac{x - iy}{1 + z}, \quad \phi_2^{-1}(q) = \left(\frac{2\Re(q)}{1 + |\zeta|^2}, \frac{-2\Im(q)}{1 + |\zeta|^2}, \frac{1 - |\zeta|^2}{1 + |\zeta|^2}\right)$$

The domains U_1 and U_2 cover S^2, and their overlap is $U_{12} = S^2\backslash\{N, S\}$. The transition map $T_{12} = \phi_2 \circ \phi_1^{-1}$ on $\mathbb{C}\backslash\{0\}$ is computed as follows:

Given $w \in \mathbb{C}\backslash\{0\}$, let $(x, y, z) = \phi_1^{-1}(p)$. Then

$$x - iy = \frac{2\bar{w}}{1 + |w|^2}, \quad 1 + z = \frac{2|w|^2}{1 + |w|^2}$$

so

$$T_{12}(p) = \phi_2(x, y, z) = \frac{x - iy}{1 + z} = \frac{\bar{w}}{|w|^2} = \frac{1}{w}$$

which is holomorphic on $\mathbb{C}\backslash\{0\}$. Similarly, $T_{21} = \phi_1 \circ \phi_2^{-1}(q) = 1/\zeta$ is holomorphic.

Thus, this atlas defines a complex structure on S^2 with holomorphic transition maps, making it a Riemann surface isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. □

Problem 1.50. *Show that the map $SL_2(\mathbb{R})/SO_2(\mathbb{R}) \xrightarrow{\sim} \mathbb{H}$ is a bijection where $SL_2(\mathbb{R}) \circlearrowright \mathbb{H}$ by*

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

Solution. Let $G = \mathrm{SL}_2(\mathbb{R})$ and $X = \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, the action $A \cdot z = \frac{az+b}{cz+d}$ maps $\mathbb{H}$ to itself, since

$$\mathrm{Im}(A \cdot z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0.$$

Define the map $\Phi : G/G_i \to \mathbb{H}$ by $\Phi([A]) = A \cdot i$. Additionally, we know that $G_i = \mathrm{SO}(2)$, so $\Phi : G/\mathrm{SO}(2) \to \mathbb{H}$. By the Orbit-Stabilizer Theorem, the map Φ is a bijection onto the orbit $G \cdot i$. Since the action is transitive, $G \cdot i = \mathbb{H}$, so Φ is a bijection.

Well-defined: If $[A] = [B]$, then $B^{-1}A \in \mathrm{SO}(2)$, so $(B^{-1}A) \cdot i = i$, and thus $A \cdot i = B \cdot i$, hence $\Phi([A]) = \Phi([B])$.

Surjective: For any $z = x + iy \in \mathbb{H}$, define

$$A_z = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \in G.$$

Then $A_z \cdot i = z$, so every $z \in \mathbb{H}$ is in the image.

Injective: If $\Phi([A]) = \Phi([B])$, then $A \cdot i = B \cdot i \Rightarrow B^{-1}A \cdot i = i$, so $B^{-1}A \in \mathrm{SO}(2) \Rightarrow [A] = [B]$.

Therefore, Φ is a well-defined bijection.

□

2 Tuesday. June 3

2.1 AM Session 1: Group Presentations

Consider the group $G = \mathbb{Z}^2$, which can be viewed as the set of lattice points in the infinite two-dimensional grid. Define the actions of a and b on $\mathbb{Z}^2$ by

$$a(x, y) = (x + 1, y), \quad b(x, y) = (x, y + 1),$$

representing unit steps in the x- and y-directions, respectively. These can be interpreted as generators corresponding to translations along the coordinate axes.

The actions of a and b commute. That is, applying a then b yields the same result as applying b then a, so we have the relation $ab = ba$. This commutativity allows us to write expressions like

$$abab = aabb = a^2b^2.$$

Thus, the group $\mathbb{Z}^2$ admits the following presentation in terms of generators and relations:

$$\mathbb{Z}^2 \cong \langle a, b \mid ab = ba \rangle.$$

Definition 2.1. *A group G is **generated** by a subset $S \subseteq G$ if no proper subgroup of G contains S.*

This definition is equivalent to the statement that every element $g \in G$ can be expressed as a finite product of elements of S and their inverses. The set of all such finite products forms the smallest subgroup of G containing S.

Example 2.2. *The group $\mathbb{Z}^2$ is generated by $S = \{(1, 0), (0, 1)\}$. However, it is not generated by $T = \{(1, 0), (0, 2)\}$. The subgroup generated by T is $\langle T \rangle = \{m(1, 0) + n(0, 2) \mid m, n \in \mathbb{Z}\} = \mathbb{Z} \times 2\mathbb{Z}$. This is a proper subgroup of $\mathbb{Z}^2$, as it fails to contain elements like $(0, 1)$.*

Definition 2.3. *A group G is generated by S if and only if every $g \in G$ can be expressed as a finite product of elements of S and their inverses.*

Example 2.4. *We explore generating sets for other familiar groups.*

1. *Find a generating set $\{a, b\}$ for $(\mathbb{Z}, +)$ such that neither a nor b alone generates $\mathbb{Z}$.*
2. *Find a generating set for $(\mathbb{Q}, +)$. Can this set be finite?*

Solution.

1. For the group $(\mathbb{Z}, +)$, the set $\{2, 3\}$ is a valid generating set. Neither element generates $\mathbb{Z}$ on its own, as $\langle 2 \rangle = 2\mathbb{Z}$ and $\langle 3 \rangle = 3\mathbb{Z}$ are proper subgroups. However, by Bézout's identity, since $\gcd(2, 3) = 1$, there exist integers x, y such that $2x + 3y = 1$. Specifically, $3 - 2 = 1$. Since 1 is an element of $\langle 2, 3 \rangle$, and 1 generates all of $\mathbb{Z}$, we have $\langle \{2, 3\} \rangle = \mathbb{Z}$.

2. For the group $(\mathbb{Q}, +)$, a generating set is given by the infinite set $S = \{\frac{1}{k} \mid k \in \mathbb{N}, k \geqslant 1\}$. Any rational number a/b can be written as an integer multiple of an element in this set, namely $a \cdot (1/b)$. No finite set $\{q_1, \ldots, q_m\}$ can generate $\mathbb{Q}$. To see this, let $q_i = a_i/b_i$ be the generators written in reduced form. Any element in the subgroup $\langle q_1, \ldots, q_m \rangle$ is of the form $\sum z_i q_i$ for $z_i \in \mathbb{Z}$. When brought to a common denominator, the denominator of such a sum must divide the least common multiple of $\{b_1, \ldots, b_m\}$. Thus, a rational number whose reduced form has a prime factor in its denominator not present in any of the b_i cannot be generated.

□

Definition 2.5. *A **word** in letters a and b is a finite string (sequence) of symbols from the set $\{a, a^{-1}, b, b^{-1}\}$.*

Example 2.6. *An example of a word is $aaba^{-1}ab^{-1}b^{-1}a^{-1}$.*

Definition 2.7. *A word is **reduced** if it contains no adjacent pairs of the form aa^{-1}, $a^{-1}a$, bb^{-1}, or $b^{-1}b$.*

Proposition 2.8. *Every word can be transformed into a unique reduced word by iteratively canceling adjacent inverse pairs.*

Example 2.9. *The word $aaba^{-1}ab^{-1}b^{-1}a^{-1}$ reduces as follows:*

$$\begin{aligned} aaba^{-1}ab^{-1}b^{-1}a^{-1} &\to aab(a^{-1}a)b^{-1}b^{-1}a^{-1} \\ &\to aabb^{-1}b^{-1}a^{-1} \\ &\to aa(bb^{-1})b^{-1}a^{-1} \\ &\to aab^{-1}a^{-1} \end{aligned}$$

The reduced form is $aab^{-1}a^{-1}$.

Reduced words can be multiplied by concatenating them and then reducing the resulting word.

Example 2.10. *The product of $(abaab^{-1})$ and (bab) is:*

$$\begin{aligned} (abaab^{-1})(bab) &= abaa(b^{-1}b)ab \\ &= aba^3b \end{aligned}$$

Definition 2.11. *The **free group of rank 2**, denoted F_2, is the group of all reduced words in two letters (say, a and b) under the operation of concatenation followed by reduction. The identity element is the empty word. The inverse of a word is obtained by reversing the order of its symbols and replacing each symbol with its inverse (e.g., the inverse of $s_1 s_2 \ldots s_k$ is $s_k^{-1} \ldots s_2^{-1} s_1^{-1}$).*

Definition 2.12. *Given any set S (of symbols or generators), one can form the **free group** $F(S)$. Its elements are reduced words formed from symbols $s \in S$ and their formal inverses s^{-1}. The group operation is concatenation followed by reduction.*

Proposition 2.13 (Universal Property of Free Groups)**.** *If G is any group, S is a set of generators, and $f : S \to G$ is any function mapping the generators to elements of G, then there exists a unique homomorphism $\varphi : F(S) \to G$ such that $\varphi(s) = f(s)$ for all $s \in S$.*

Example 2.14. *If $w = a^2b^{-1}a$ is an element of $F(\{a, b\})$, and $f : \{a, b\} \to G$ is a function, then the homomorphism φ acts as:*

$$\begin{aligned}\varphi(a^2b^{-1}a) &= \varphi(a)\varphi(a)\varphi(b^{-1})\varphi(a)\\ &= f(a) \cdot f(a) \cdot f(b)^{-1} \cdot f(a)\end{aligned}$$

The primary task in proving the proposition is to show that φ defined in this manner is a well-defined homomorphism (i.e., respects the group operation).

2.2 AM Session 2: Trees

Recall that $\mathbb{Z}^2 \cong \langle a, b \mid ab = ba\rangle$.

Example 2.15. *Let $S = \{a, b\}$ be a set of formal generators. We can define a function $f : S \to \mathbb{Z}^2$ by $f(a) = (1, 0)$ and $f(b) = (0, 1)$. By the universal property of free groups, this function extends to a homomorphism from the free group $F_2 = F(S)$ to $\mathbb{Z}^2$.*

Exercise 2.16. *Let $\varphi : F_2 \to \mathbb{Z}^2$ be the homomorphism extending $f(a) = (1, 0)$ and $f(b) = (0, 1)$. Determine the image $im(\varphi)$ and the kernel $ker(\varphi)$.*

Solution. The homomorphism φ is surjective, so its image $\mathrm{im}(\varphi)$ is all of $\mathbb{Z}^2$. This is because any element $(m, n) \in \mathbb{Z}^2$ can be written as $m(1, 0) + n(0, 1)$, which is $\varphi(a^m b^n)$ (where $a^m b^n$ is an element of F_2). By the First Isomorphism Theorem, we have $\mathbb{Z}^2 \cong F_2/\ker(\varphi)$.

The kernel, $\ker(\varphi)$, consists of all words $w \in F_2$ such that $\varphi(w) = (0, 0)$. This is the smallest normal subgroup $N \trianglelefteq F_2$ such that the quotient F_2/N is abelian. □

Definition 2.17. *The **normal closure** of a subset $X \subseteq G$ in a group G, denoted $\langle\langle X\rangle\rangle$, is the intersection of all normal subgroups of G that contain X. It is the smallest normal subgroup of G containing X.*

Exercise 2.18. *Show that the normal closure $\langle\langle X\rangle\rangle$ is the subgroup generated by all conjugates of elements of X and their inverses. That is, $\langle\langle X\rangle\rangle$ is generated by the set $\{gx^{\pm 1}g^{-1} \mid x \in X, g \in G\}$.*

Example 2.19. *The commutator $aba^{-1}b^{-1}$ is an element of $ker(\varphi)$ because $\varphi(aba^{-1}b^{-1}) = f(a) + f(b) - f(a) - f(b) = (1, 0) + (0, 1) - (1, 0) - (0, 1) = (0, 0)$. Therefore, the normal closure $N = \langle\langle\{aba^{-1}b^{-1}\}\rangle\rangle$ must be a subgroup of $ker(\varphi)$, i.e., $N \subseteq ker(\varphi)$.*

Lemma 2.20. *Let $c = aba^{-1}b^{-1}$ and $N = \langle\langle\{c\}\rangle\rangle$. A conjugate of c, such as $a^{-1}ca = a^{-1}(aba^{-1}b^{-1})a = ba^{-1}b^{-1}a$, is in N. The inverse $c^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$ is also in N. More generally, N contains all elements that can be formed by products of conjugates of c and c^{-1}. The claim is that elements like $[a, b^{-1}] = ab^{-1}a^{-1}b$, $[b^{-1}, a^{-1}] = b^{-1}a^{-1}ba$, and $[a^{-1}, b] = a^{-1}bab^{-1}$ are also in this specific N.*

Exercise 2.21. *Let φ be a group homomorphism and suppose $N \trianglelefteq G$ is a normal subgroup such that $\ker(\varphi) \subseteq N$. Given an element $w \in \ker(\varphi)$, show that w can be transformed, via conjugation and multiplication by elements of N, into an element of N. Conclude that $w \in N$.*

Proof. We present the proof idea by working through an example and then indicate how it generalizes. Consider the word

$$w = a^2b^{-1}a^{-3}ba \in \ker(\varphi).$$

Our goal is to reduce this to an element of N using conjugation and multiplication by elements of N.

Observe that we can regroup and conjugate strategically:

$$w = a^2b^{-1}a^{-3}ba = a \cdot (ab^{-1}a^{-1}) \cdot a^{-2}ba.$$

Now we apply conjugation:

$$ab^{-1}a^{-1} = (aba^{-1})^{-1},$$

so the term $ab^{-1}a^{-1}$ is a conjugate of b^{-1}, and since conjugation preserves membership in N (because N is normal), it lies in N if b^{-1} does.

Continuing:

$$w = a \cdot (ab^{-1}a^{-1}) \cdot a^{-2}ba.$$

Focus on reducing the powers of a while preserving group equivalence modulo N. Note that:

$$a^{-3}ba = a^{-2}(a^{-1}ba) = a^{-2} \cdot b',$$

where $b' = a^{-1}ba$ is a conjugate of b, hence lies in N if $b \in N$.

By applying this reasoning recursively (each step reducing the number of a's), we eventually rewrite w as a product of conjugates of $b^{\pm 1}$ and powers of a that cancel or combine, producing an element in N.

Since all intermediate steps involve conjugation and elements of N, and N is closed under these operations, the result lies in N. Hence, $w \in N$. □

The upshot of this (that $\ker(\varphi) = \langle\langle\{aba^{-1}b^{-1}\}\rangle\rangle$) is that

$$\mathbb{Z}^2 \cong F_2/\langle\langle aba^{-1}b^{-1}\rangle\rangle.$$

Definition 2.22. *A **presentation** of a group G is an isomorphism $G \cong \langle S \mid R \rangle$. Here, S is a set of generators, and R is a set of relations (words in $F(S)$, the free group on S). The notation $\langle S \mid R \rangle$ denotes the quotient group $F(S)/\langle\langle R \rangle\rangle_{F(S)}$, where $\langle\langle R \rangle\rangle_{F(S)}$ is the normal closure of R in $F(S)$. This normal closure is the kernel of the canonical surjective homomorphism $\pi : F(S) \to G$ defined by mapping generators in S to their corresponding elements in G.*

Example 2.23. *$\mathbb{Z}/n\mathbb{Z} \cong \langle a \mid a^n \rangle$. Here $S = \{a\}$ and $R = \{a^n\}$.*

Example 2.24. *$\mathbb{Z}^2 \cong \langle a, b \mid aba^{-1}b^{-1} \rangle$. Here $S = \{a, b\}$ and $R = \{aba^{-1}b^{-1}\}$. The relation $aba^{-1}b^{-1} = e$ is equivalent to $ab = ba$.*

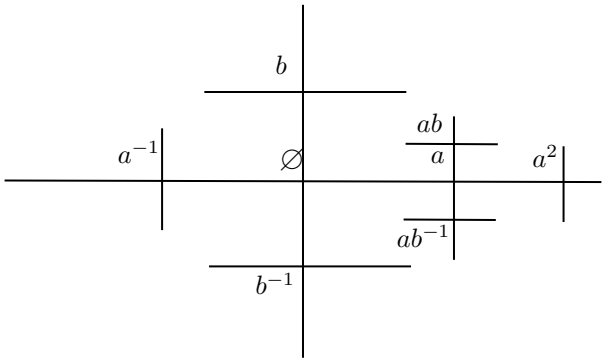
If we write down some random generators and relations, we define a group. However, it can be very difficult to understand the properties of the group, such as whether it is trivial, finite, infinite, abelian, etc. The word problem for groups (determining if a given word in the generators represents the identity element) is, in general, undecidable (Novikov-Boone theorem). This implies there's no general algorithm to determine if a finitely presented group is trivial. The goal, then, often becomes to find "good" presentations for known groups or to develop tools to analyze groups given by their presentations. One such powerful tool is the theory of group actions on trees.

Definition 2.25. *A **graph** Γ consists of a set of vertices $V(\Gamma)$, a set of edges $E(\Gamma)$, and an endpoint function that maps each edge $e \in E(\Gamma)$ to an unordered pair of vertices $\{u, v\}$ from $V(\Gamma)$ (its endpoints). If $u = v$, the edge is a loop. Multiple edges can connect the same pair of vertices.*

Definition 2.26. *A **tree** is a connected graph that contains no simple cycles (i.e., no path that starts and ends at the same vertex without retracing edges or visiting other vertices multiple times, apart from the start/end vertex).*

Trees are fundamentally related to free groups.

Consider the free group F_2 on generators $S = \{a, b\}$. We can construct its Cayley graph, denoted here as T_2: The set of vertices $V(T_2)$ is the set of elements of F_2. Two vertices $v, w \in F_2$ are connected by an edge if $w = vs$ in F_2 for some $s \in \{a, b, a^{-1}, b^{-1}\}$. (Here vs means the product in F_2, which is already a reduced word if v does not end in s^{-1}; otherwise, cancellation occurs). Each edge can be labeled by the generator s used.



This graph T_2 is the Cayley graph of F_2 with respect to the generators $\{a, b\}$.

Exercise 2.27. *Show that this graph T_2 is a tree.*

The group F_2 acts on its Cayley graph T_2. This action is defined on vertices by left multiplication: if $g \in F_2$ and $v \in V(T_2) = F_2$, then $g \cdot v = gv$ (product in F_2). This action extends to edges: if $e = (v, vs')$ is an edge (where $s' \in \{a, b, a^{-1}, b^{-1}\}$), then $g \cdot e = (gv, gvs')$. This action respects the graph structure (adjacency and endpoints).

This action is free on vertices (if $g \cdot v = v$, then $gv = v$, which implies $g = e$ since F_2 is a group). It is also free on oriented edges. Furthermore, the action is transitive on vertices (for any $v_1, v_2 \in F_2$, there exists $g = v_2 v_1^{-1} \in F_2$ such that $g \cdot v_1 = v_2$).

Theorem 2.28. *A group G is isomorphic to a free group if and only if it acts freely on a tree.*

2.3 AM Problem Session

Problem 2.29. *Prove that a group G is generated by a subset S if and only if every element of G can be obtained by multiplying elements of S and their inverses, with reptition.*

Solution. Let H be the set of all finite products of elements of S and their inverses. We first show H is a subgroup of G. The empty product is the identity $\varnothing$, so $\varnothing \in H$. If $h = s_1^{\varnothing_1} \dots s_k^{\varnothing_k} \in H$, then its inverse $h^{-1} = s_k^{-\varnothing_k} \dots s_1^{-\varnothing_1}$ is also a finite product of elements from $S \cup S^{-1}$, so $h^{-1} \in H$. Closure under multiplication is clear from the definition. Thus H is a subgroup of G. By construction, $S \subseteq H$.

Now, let $\langle S \rangle$ be the subgroup generated by S, defined as the intersection of all subgroups of G containing S. Since H is one such subgroup, we must have $\langle S \rangle \subseteq H$. Conversely, any subgroup containing S must be closed under multiplication and inverses, so it must contain all elements of H. Therefore, $H \subseteq \langle S \rangle$. We conclude that $H = \langle S \rangle$.

The statement that G is generated by S means $\langle S \rangle = G$. By the above, this is equivalent to every element of G being an element of H, i.e., a finite product of elements from S and their inverses. □

Problem 2.30. *For each natural number n, find a generating set S of the group $\mathbb{Z}$ of cardinality n such that no subset generates $\mathbb{Z}$.*

Solution. Let $n \geqslant 2$. Let $p_1, \ldots, p_n$ be distinct prime numbers. Define $s_i = \prod_{j \neq i} p_j$ for $i = 1, \ldots, n$. Let $S = \{s_1, \ldots, s_n\}$. The greatest common divisor of the set S is $\gcd(s_1, \ldots, s_n) = 1$, because no single prime p_k divides all the elements s_i (specifically, p_k does not divide s_k). By the extended Euclidean algorithm, the subgroup $\langle S \rangle$ is $d\mathbb{Z}$ where $d = \gcd(S)$. Since $d = 1$, $\langle S \rangle = \mathbb{Z}$. Now consider any proper subset $S' \subset S$. Let s_k be an element not in S'. Then every element in S' is a multiple of the prime p_k. Thus, any integer combination of elements from S' will also be a multiple of p_k. The subgroup generated by S' is therefore contained in $p_k\mathbb{Z}$, which is a proper subgroup of $\mathbb{Z}$. Thus, no proper subset of S generates $\mathbb{Z}$. □

Problem 2.31. *Prove that every finitely generated group G is countable. Prove that, if G is a finitely generated group and H is a finite (resp. countable) group, then there are finitely many (resp. countably many) homomorphisms $G \to H$.*

Solution. Let G be generated by a finite set $S = \{s_1, \ldots, s_n\}$. Every element of G can be written as a finite word in the alphabet $A = S \cup S^{-1}$, which has size $2n$. The set of all words of length k is finite, $|A|^k$. The set of all finite words is a countable union of finite sets, $\cup_{k=0}^{\infty} A^k$, and is therefore countable. Since there is a surjective map from the set of all words to the group G, the group G must be at most countable. As infinite groups exist, G is countable.

A homomorphism $\varphi : G \to H$ is uniquely determined by its values on the generating set S. For each generator $s_i \in S$, its image $\varphi(s_i)$ must be an element of H. There are $|H|$ choices for each $\varphi(s_i)$. This defines a function from S to H. By the universal property, this function extends to a unique homomorphism from the free group $F(S)$ to H. For this to descend to a homomorphism from $G = F(S)/\langle\langle R \rangle\rangle$, the images of the generators in H must satisfy the relations R. Regardless, the total number of possible ways to map the generators is $|H|^n$.

1. If H is finite, there are at most $|H|^n$ (a finite number) of homomorphisms from G to H.
2. If H is countable, there are at most $|H|^n = \aleph_0^n = \aleph_0$ (a countable number) of homomorphisms.

This solves the problem. □

Problem 2.32.

1. *Prove that every word in a and b can be reduced to a unique reduced word. Hint: prove by induction on length of words that two different choices of reduction will both lea to the same reduced word.*

2. *Carefully check that the free group F_2 is a group. Hint: For associativity, you will want to use the previous exercise.*

Solution.

1. We use induction on the length of a word w. The base case, a word of length 0 or 1, is already reduced. Assume any two sequences of reductions on a word of length less than k lead to the same reduced word. Let w be a word of length k. Suppose we apply two different reduction steps. If the reductions occur at disjoint positions (e.g., $w = w_1ss^{-1}w_2tt^{-1}w_3$), then reducing either pair first leads to an intermediate word of length $k-2$, and reducing the other pair from there leads to the same result. The only difficult case is overlapping reductions, i.e., $w = uss^{-1}sv$. One reduction gives usv. The other gives $us^{-1}sv$. Both of these words are of length $k-1$. By the inductive hypothesis, they both reduce to the same unique word. This establishes that any two reduction paths of one step can be joined. A simple induction on the number of steps completes the proof that all reduction sequences terminate at the same unique reduced word.

2. Let the operation be concatenation followed by reduction, denoted by $*$.

3. Closure: The product of two reduced words is, after concatenation and reduction, another reduced word. So the set is closed.

   Identity: The empty word $\varnothing$ serves as the identity. For any reduced word w, $w * \varnothing = w$ and $\varnothing * w = w$ since no reductions are possible.

   Inverse: For a reduced word $w = s_1s_2 \dots s_k$, its inverse is $w^{-1} = s_k^{-1} \dots s_2^{-1}s_1^{-1}$. Their concatenation ww^{-1} reduces completely to $\varnothing$.

   Associativity: We must show $(u*v)*w = u*(v*w)$ for any reduced words u, v, w. Let $u \cdot v \cdot w$ denote the word formed by simple concatenation. Then $(u*v)*w$ is the unique reduced form of the word $(u \cdot v)_r \cdot w$, where $(u \cdot v)_r$ is the reduced form of $u \cdot v$. Similarly, $u * (v * w)$ is the unique reduced form of $u \cdot (v \cdot w)_r$. By the uniqueness of reduced forms (Part 1), both of these must be equal to the unique reduced form of the word $u \cdot v \cdot w$. Therefore, associativity holds.

□

Problem 2.33. *Let D_n be the dihedral group with $2n$ elements, the group of rigid motions of the plane preserving a regular n-gon. Show that D_n has the presentation*

$$\langle s, t | s^n, t^2, stst \rangle$$

Hint: Think of this in two steps. First find generators s and t that satisfy the given relations, which says that D_n is a quotient of the group with the given presentation. Then show that D_n is no smaller, with a cardinality argument.

Solution. Let $G = \langle s, t | s^n, t^2, stst \rangle$. Let D_n be the group of symmetries of a regular n-gon. We can identify a generator for rotations, say ρ (rotation by $2\pi/n$), and a generator for reflections, say τ (reflection across a chosen axis). These satisfy the relations $\rho^n = \text{id}$, $\tau^2 = \text{id}$, and $\tau\rho\tau^{-1} = \rho^{-1}$. Since $\tau = \tau^{-1}$, this last relation is $\tau\rho\tau = \rho^{-1}$, or $\tau\rho\tau\rho = \text{id}$. By the universal property, the map $f : \{s, t\} \to D_n$ given by $f(s) = \rho$ and $f(t) = \tau$ extends to a group homomorphism $\varphi : G \to D_n$. Since ρ and τ generate D_n, the homomorphism φ is surjective.

Now we examine the size of G. The relations $t^2 = e$ and $stst = e \implies st = t^{-1}s^{-1} = ts^{-1}$ allow any word in G to be written in the form $s^i t^j$ for integers i, j. The relation $s^n = e$ restricts i to $\{0, 1, \ldots, n-1\}$, and $t^2 = e$ restricts j to $\{0, 1\}$. Thus, there are at most $2n$ distinct elements in G. We have a surjective homomorphism $\varphi : G \to D_n$, where $|G| \leqslant 2n$ and $|D_n| = 2n$. A surjective map from a set of size at most m to a set of size m must be a bijection. Therefore, φ is an isomorphism, and $G \cong D_n$. □

Problem 2.34. *Consider groups defined by the following presentations:*

$$G_2 = \langle a, b | aba^{-1}b^{-2}, bab^{-1}a^{-2} \rangle$$
$$G_3 = \langle a, b, c | aba^{-1}b^{-2}, bcb^{-1}c^{-2}, cdc^{-1}d^{-2}, dad^{-1}a^{-2} \rangle$$
$$G_4 = \langle a, b, c, d | aba^{-1}b^{-2}, bcb^{-1}c^{-2}, cdc^{-1}d^{-2}, dad^{-1}a^{-2} \rangle$$

Show that both G_2 and G_3 are the trivial group. Then, show that G_4 is not trivial.

Solution. These are the Higman groups.

Case $n = 2$: $G_2 = \langle a, b | aba^{-1} = b^2, bab^{-1} = a^2 \rangle$. From the first relation, $a = b^2ab^{-1}$. From the second, $a^2 = bab^{-1}$. Substitute a^2 into the first relation: $aba^{-1} = b(bab^{-1})b^{-1} = ba$. This implies $aba^{-1} = ba \implies ab = ba^2$. But from $bab^{-1} = a^2$, we have $ba = a^2b$. So $ab = a^2b$, which gives $a = a^2$, so $a = e$. If $a = e$, the second relation $bab^{-1} = a^2$ gives $e = e$, and the first relation $aba^{-1} = b^2$ gives $b = b^2$, so $b = e$. Thus G_2 is the trivial group.

Case $n = 3$: I don't know how to do this.

Case $n = 4$: I don't know how to do this.

□

Problem 2.35. *Check that the following are equivalent for a connected graph Γ:*

1. Γ *contains no cycle as a subgraph.*
2. *Any two vertices in* Γ *are connected by a unique non-backtracking edge path.*
3. *Removing any edge of* Γ *disconnects the graph.*

Solution. $(1 \Rightarrow 2)$ Since Γ is connected, there exists at least one path between any two vertices u, v. Suppose there were two distinct paths, P_1 and P_2. Let x be the first vertex on P_1 (starting from u) that is not on P_2 (or where the paths diverge), and let y be the first vertex after x on P_1 that is also on P_2. The segment of P_1 from x to y and the segment of P_2 from x to y form a cycle. This contradicts (1). Thus, the path must be unique.

$(2 \Rightarrow 3)$ Let $e = \{u, v\}$ be an edge in Γ. This edge itself is a path from u to v. By (2), this is the only path between u and v. If we remove e, there is no longer any path between u and v, so the graph becomes disconnected.

$(3 \Rightarrow 1)$ Assume, for contradiction, that Γ contains a cycle C. Let $e = \{u, v\}$ be any edge on this cycle. The remaining edges of the cycle, $C \backslash \{e\}$, form a path between u and v. Therefore, removing the edge e does not disconnect the graph, as u and v (and all other vertices) remain connected through the rest of the cycle. This contradicts (3). Thus, Γ must contain no cycles.

□

Problem 2.36. *Check that the Cayley graph of the group group* F_2 *is a tree. Describe the actions of each generator on the tree.*

Solution. Let Γ be the Cayley graph of $F_2 = \langle a, b \rangle$. The vertices are the elements of F_2. By definition, Γ is connected. To show it is a tree, we must show it contains no cycles. A path starting and ending at a vertex g corresponds to a sequence of generators $s_1, \ldots, s_k$ such that $gs_1s_2 \ldots s_k = g$. This implies the word $w = s_1 \ldots s_k$ represents the identity element in F_2. In a free group, the only word that represents the identity is a word that is not freely reduced (i.e., it reduces to the empty word). A cycle is a path that does not retrace edges. A non-retracing path in the Cayley graph corresponds to a freely reduced word. Since no non-empty freely reduced word is equal to the identity, there are no cycles in Γ. Thus, the Cayley graph of F_2 is a tree.

The group F_2 acts on this tree by left multiplication. Let $g \in F_2$. The action of a generator, say a, maps every vertex v to the vertex av. Geometrically, this action is a "translation" along the paths composed of a-edges. Every vertex is moved one unit along the unique outgoing a-edge. The action of a^{-1} is the inverse translation. The action has no global fixed points; it moves the entire infinite tree without rotation or reflection about any point. □

2.4 PM Lecture 1: Riemann Surfaces III

Yesterday, our aim was to classify all Riemann surfaces, with a particular focus on compact Riemann surfaces.

If X is a compact Riemann surface, then topologically X is also a compact, connected, orientable two-dimensional real manifold. So, we start with a compact Riemann surface. Applying a "forgetful" map that discards the complex structure leaves us with such a manifold. These underlying topological manifolds are classified by their genus $g \in \mathbb{Z}_{\geqslant 0}$ (a non-negative integer).

In the genus $g = 0$ case, the underlying topological space is the 2-sphere S^2. We've already seen that S^2 admits a unique complex structure (up to biholomorphism), making it the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$. Hence, the fiber of the forgetful map over S^2 (i.e., the set of distinct complex structures on S^2) is a singleton set.

Exercise 2.37.

1. *Show that $\mathbb{C}^\times$ acts on $\mathbb{C}^{n+1}\backslash\{0\}$ by scalar multiplication:*

$$\lambda \cdot (x_0, x_1, \ldots, x_n) = (\lambda x_0, \lambda x_1, \ldots, \lambda x_n).$$

2. *The complex projective n-space $\mathbb{P}^n_{\mathbb{C}}$ is defined as the quotient space*

$$(\mathbb{C}^{n+1}\backslash\{0\})/\mathbb{C}^\times$$

   under this action. Show that $\mathbb{P}^1_{\mathbb{C}}$ is a Riemann surface.

3. *Show that $\mathbb{P}^1_{\mathbb{C}}$ is homeomorphic to S^2 as topological spaces.*

Note: Coordinates on $\mathbb{P}^n_{\mathbb{C}}$ will be denoted by $[x_0 : x_1 : \cdots : x_n]$.

In the genus $g = 1$ case, the underlying topological space is the torus $S^1 \times S^1$. The set of distinct complex structures on the torus (i.e., the fiber of the forgetful map over $S^1 \times S^1$) is parameterized by homothety classes of lattices in $\mathbb{C}$. (Homothety means scaling by a non-zero complex number).

A lattice $\Lambda \subseteq \mathbb{C}$ is a $\mathbb{Z}$-submodule of the form $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, where $w_1, w_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent complex numbers. Two lattices Λ and Λ' are considered equivalent (or in the same homothety class) if $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C}^\times$. We saw yesterday that the quotient $\mathbb{C}/\Lambda$ forms a Riemann surface of genus 1.

Consider ordered pairs (w_1, w_2) of non-zero complex numbers. We define a map Z by $Z(w_1, w_2) = \frac{w_1}{w_2} \in \mathbb{C} \cup \{\infty\}$. If w_1, w_2 are restricted to be $\mathbb{R}$-linearly independent, then $Z(w_1, w_2)$ maps to $\mathbb{H}^+ \sqcup \mathbb{H}^- = \mathbb{C}\backslash\mathbb{R}$ (the union of the upper and lower half-planes). The map Z is invariant under homothety: $Z(\alpha w_1, \alpha w_2) = Z(w_1, w_2)$ for $\alpha \in \mathbb{C}^\times$. Thus, the set of homothety classes of ordered pairs of $\mathbb{R}$-linearly independent complex numbers is identified with $\mathbb{H}^+ \sqcup \mathbb{H}^-$.

Exercise 2.38. *Let $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ be a lattice in $\mathbb{R}^2$.*

1. *Show that for any matrix*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R}),$$

the action

$$A \cdot \Lambda := \mathbb{Z}(aw_1 + bw_2) \oplus \mathbb{Z}(cw_1 + dw_2)$$

defines a well-defined action of $\mathrm{GL}_2(\mathbb{R})$ on the space of lattices in $\mathbb{R}^2$.

2. *Show that the action*

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

is a well-defined action of $\mathrm{GL}_2(\mathbb{R})$ on the extended upper half-plane $\mathbb{H}^+ \sqcup \mathbb{H}^-$.

3. *Show that the stabilizer of the point $i \in \mathbb{H}^+$ under this action is the orthogonal group $\mathrm{O}_2(\mathbb{R})$. Deduce that there is a bijection*

$$\mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R}) \cong \mathbb{H}^+ \sqcup \mathbb{H}^-.$$

So, we have a correspondence: the set of homothety classes of ordered, $\mathbb{R}$-linearly independent pairs (w_1, w_2) can be identified with $Z(w_1, w_2) \in \mathbb{H}^+ \sqcup \mathbb{H}^- \cong \mathrm{GL}_2(\mathbb{R})/\mathrm{O}_2(\mathbb{R})$. Furthermore, the set of homothety classes of such pairs (w_1, w_2) surjects onto the set of homothety classes of lattices in $\mathbb{C}$.

This relationship can be summarized in the following diagram:

$$\begin{array}{ccc} \text{pairs of } \mathbb{R}\text{-independent complex numbers up to homothety} & \xrightarrow{\quad Z \quad} & \mathrm{GL}_2(\mathbb{R})/O_2(\mathbb{R}) \\ \Big\downarrow & & \Big\downarrow \\ \{\text{space of all lattices in } \mathbb{C}\} & \xrightarrow[Z]{\sim} & \mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})/O_2(\mathbb{R}) \end{array}$$

The map Z gives the isomorphism between the space of homothety classes of lattices and the double coset space.

Exercise 2.39.

1. *Show that the action of $GL_2(\mathbb{Z})$ (as a subgroup of $GL_2(\mathbb{R})$) on $GL_2(\mathbb{R})/O_2(\mathbb{R}) \cong \mathbb{H}^+ \sqcup \mathbb{H}^-$ corresponds to the action $z \mapsto \frac{az+b}{cz+d}$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$.*

2. *Show that $GL_2(\mathbb{Z})\backslash(\mathbb{H}^+ \sqcup \mathbb{H}^-) \cong SL_2(\mathbb{Z})\backslash\mathbb{H}^+$.*

We have thus identified the space of homothety classes of lattices in $\mathbb{C}$ with $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$. This space is denoted $X(1)$ (where $\Gamma(1)$ is another name for $\mathrm{SL}_2(\mathbb{Z})$). $X(1)$ is a non-compact Riemann surface, biholomorphic to $\mathbb{C}$.

Proposition 2.40.

$X(1)$ has a standard compactification $Y(1)$,, which is also a Riemann surface. In fact, $Y(1)$ is biholomorphic to the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$. The compactification adds one point (a cusp): $Y(1) \backslash X(1) = \{\infty\}$.

Now we move on to briefly introduce projective varieties. Recall that $\mathbb{P}^n_{\mathbb{C}} := (\mathbb{C}^{n+1} \backslash \{0\})/\mathbb{C}^\times$. In affine spaces like $\mathbb{C}^k$ (analogous to $\mathbb{R}^k$), we study affine varieties (and more generally, manifolds). In projective spaces $\mathbb{P}^n_{\mathbb{C}}$, we study projective varieties.

We now briefly introduce *projective varieties*. Recall that the complex projective space of dimension n, denoted $\mathbb{P}^n_{\mathbb{C}}$, is defined as the set of equivalence classes

$$\mathbb{P}^n_{\mathbb{C}} := \left(\mathbb{C}^{n+1} \backslash \{0\}\right) / \sim,$$

where two nonzero vectors $(x_0, \ldots, x_n)$ and $(y_0, \ldots, y_n)$ in $\mathbb{C}^{n+1}$ are equivalent, written $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$, if there exists a nonzero scalar $\lambda \in \mathbb{C}$ such that $(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n)$.

In real Euclidean space $\mathbb{R}^n$, we often study manifolds defined by real-valued equations. In contrast, in the projective setting, particularly in $\mathbb{P}^n_{\mathbb{C}}$, we study *projective varieties*, which are the zero sets of homogeneous polynomials in $\mathbb{C}[x_0, \ldots, x_n]$.

As an example, consider the affine equation

$$x^2 + y^2 + z^2 = 1.$$

This defines a surface in $\mathbb{C}^3$, and the point $(x, y, z) = (1, 0, 0)$ is clearly a solution. However, when we pass to projective space, we must account for the equivalence relation. For instance, in $\mathbb{P}^n_{\mathbb{C}}$, the points $(1, 0, 0)$ and $(2, 0, 0)$ are considered equivalent because they differ by a scalar multiple.

To correctly define the variety in projective space, we must *homogenize* the equation. That is, we introduce a new variable w and consider the homogeneous equation

$$x^2 + y^2 + z^2 = w^2.$$

Now points like $(i, 1, 0, \sqrt{2})$ and $(2i, 2, 0, 2\sqrt{2})$ represent the same point in $\mathbb{P}^3_{\mathbb{C}}$, preserving the equivalence structure. Homogenization ensures that the variety is well-defined in projective space.

Definition 2.41. *A **projective curve** in $\mathbb{P}^2_{\mathbb{C}}$ is the set of points $[x : y : z] \in \mathbb{P}^2_{\mathbb{C}}$ such that $F(x, y, z) = 0$, where $F(x, y, z)$ is a non-constant homogeneous polynomial.*

Definition 2.42. *A projective curve defined by $F(x, y, z) = 0$ is **smooth** if the gradient vector $\nabla F = \left[\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}\right]$ is non-zero (i.e., has rank 1) at every point $[x : y : z]$ on the curve.*

Example 2.43.

1. *$F(x,y,z) = x+y+z$ defines a smooth curve because its gradient is $\nabla F = [1,1,1]$, which is never zero.*
2. *Consider $F(x,y,z) = x^2+xy+xz = x(x+y+z)$. This curve is not smooth. Its gradient is $\nabla F = [2x+y+z, x, x]$. At the point $[0:1:-1]$ (which satisfies $F(0,1,-1) = 0$), the gradient evaluated using the representative $(0,1,-1)$ is $[2(0)+1+(-1),0,0] = [0,0,0]$. Since the gradient vanishes, the curve is not smooth at $[0:1:-1]$.*

Proposition 2.44. *If $C = \{[x:y:z] \in \mathbb{P}^2_{\mathbb{C}} \mid F(x,y,z) = 0\}$ is a smooth projective curve (where F is a non-constant homogeneous polynomial), then C is a compact Riemann surface.*

2.5 PM Session 2: Elliptic Curves

Theorem 2.45.

1. *Let X be a compact, connected, orientable two-dimensional manifold (a surface). Then X can be endowed with the structure of a Riemann surface.*
2. *Any compact Riemann surface is algebraic. This means that X can be holomorphically embedded into some complex projective space $\mathbb{P}^n_{\mathbb{C}}$ as a smooth algebraic curve.*

Corollary 2.46. *For any lattice $\Lambda \subset \mathbb{C}$, the complex torus $\mathbb{C}/\Lambda$ is algebraic. That is, $\mathbb{C}/\Lambda$ can be embedded as a smooth projective algebraic curve in some $\mathbb{P}^n_{\mathbb{C}}$ (specifically, $\mathbb{P}^2_{\mathbb{C}}$ as shown below).*

Definition 2.47. *The **Weierstrass $\wp$-function** associated with a lattice Λ is defined for $z \in \mathbb{C}\backslash\Lambda$ as*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w\in\Lambda\backslash\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

This series converges uniformly on compact subsets of $\mathbb{C}\backslash\Lambda$. The function $\wp_\Lambda(z)$ is an even, doubly periodic (elliptic) function with periods in Λ, and has double poles at each lattice point.

Proposition 2.48. *The Weierstrass $\wp$-function satisfies the differential equation:*

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_2(\Lambda)$ and $g_3(\Lambda) = 140G_3(\Lambda)$. The terms $G_k(\Lambda)$ are values of Eisenstein series, defined as $G_k(\Lambda) = \sum_{w\in\Lambda\backslash\{0\}} w^{-2k}$ for integers $k > 1$ (so $2k \geqslant 4$, which ensures convergence). Thus, $g_2(\Lambda)$ uses $G_2(\Lambda) = \sum' w^{-4}$ and $g_3(\Lambda)$ uses $G_3(\Lambda) = \sum' w^{-6}$.

Theorem 2.49. *The map $\Phi : \mathbb{C}/\Lambda \to \mathbb{P}^2_{\mathbb{C}}$, defined by*

$$\Phi(z+\Lambda) = \begin{cases} [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1] & \text{if } z \notin \Lambda \\ [0:1:0] & \text{if } z \in \Lambda \end{cases}$$

is a well-defined holomorphic embedding. Its image is the projective algebraic curve C_Λ in $\mathbb{P}^2_{\mathbb{C}}[X:Y:Z]$ defined by the homogeneous equation:

$$Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3.$$

Thus, $\mathbb{C}/\Lambda$ is isomorphic as a Riemann surface to C_Λ.

Definition 2.50. *Curves in $\mathbb{P}^2_{\mathbb{C}}[X:Y:Z]$ defined by an equation of the form $Y^2Z = 4X^3 - aXZ^2 - bZ^3$ are called **elliptic curves**, provided their discriminant $\Delta = a^3 - 27b^2$ is non-zero (which ensures the curve is smooth).*

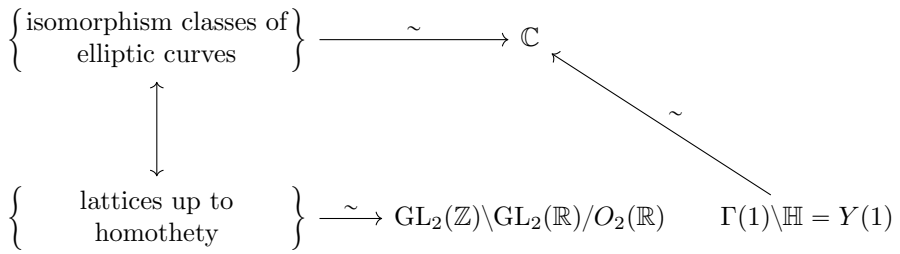
Definition 2.51. *The **j-invariant** is defined as*

$$j(E(a,b)) := 1728\frac{a^3}{\Delta},$$

where $\Delta = a^3 - 27b^2$.

Theorem 2.52. *Two elliptic curves $E(a,b)$ and $E(a',b')$ (defined by coefficients a,b and a',b' respectively) are isomorphic as Riemann surfaces (and as algebraic curves over $\mathbb{C}$) if and only if their j-invariants are equal: $j(E(a,b)) = j(E(a',b'))$.*

So, we have the following correspondences:



How does one construct the map from $Y(1)$ (representing lattices up to homothety and choice of basis orientation) to $\mathbb{P}^1_{\mathbb{C}}$ (representing isomorphism classes of elliptic curves) directly using the j-invariant? To understand this, we need to discuss modular forms and modular curves. Consider $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$, which is a subgroup of $\mathrm{SL}_2(\mathbb{R})$ and acts on the complex upper half-plane $\mathbb{H}$ by fractional linear transformations: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau+b}{c\tau+d}$.

Definition 2.53. *For an integer $N \geqslant 1$, the **principal congruence subgroup of level** N is defined as $\Gamma(N) = \ker\left(SL_2(\mathbb{Z}) \to SL_2\left(\mathbb{Z}/N\mathbb{Z}\right)\right)$.*

An element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ is in $\Gamma(N)$ if and only if $a \equiv d \equiv 1 \pmod{N}$ and $b \equiv c \equiv 0 \pmod{N}$. The quotient space $X(1) = \Gamma(1)\backslash\mathbb{H}$ is isomorphic to $\mathbb{C}$ via the j-invariant map.

We define $X(N) = \Gamma(N)\backslash\mathbb{H}$ and $Y(N)$ as its compactification. These are Riemann surfaces. Note that if M divides N, then $\Gamma(N) \subseteq \Gamma(M)$, which implies there is a natural projection map (a covering map) $Y(N) \to Y(M)$. This gives a diagram of modular curves:

$$\begin{array}{ccc} Y(2) & \longleftarrow & Y(6) \\ \downarrow & & \downarrow \\ Y(1) & \longleftarrow & Y(3) \end{array}$$

Just as $X(1)$ is compactified to $Y(1)$, similar constructions yield compact Riemann surfaces $Y(N)$ from $X(N)$ for other levels N. These $Y(N)$ are called **modular curves**.

Definition 2.54. *A **modular function of level** N (for $\Gamma(N)$) is a meromorphic function on the compact Riemann surface $Y(N)$. Equivalently, it's a function $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ such that f is meromorphic on $\mathbb{H}$, $f(\gamma \cdot \tau) = f(\tau)$ for all $\gamma \in \Gamma(N)$, and f is meromorphic at the cusps.*

Example 2.55. *The j-invariant is a modular function of level 1. It is holomorphic on $\mathbb{H}$ (and on $X(1)$), with a simple pole at the cusp ∞ of $Y(1)$.*

Note that neither $g_2(\Lambda)$ nor $g_3(\Lambda)$ (viewed as functions of τ by setting $\Lambda = \mathbb{Z}\tau \oplus \mathbb{Z}1$) is a modular function of level 1 because they are not invariant under the action of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

2.6 PM Problem Session

Problem 2.56.

1. *Show that $\mathbb{C}^\times = \mathbb{C}\backslash\{0\}$ acts on $\mathbb{C}^{n+1}\backslash\{0\}$ by $\lambda\cdot(x_0, \ldots, x_n) = (\lambda x_0, \ldots, \lambda x_n)$.*
2. *Let $\mathbb{P}^n_{\mathbb{C}} = (\mathbb{C}^{n+1}\backslash\{0\})/\mathbb{C}^\times$. Show that $\mathbb{P}^1_{\mathbb{C}}$ is a Riemann surface.*
3. *Show that $\mathbb{P}^1_{\mathbb{C}} \simeq S^2$ as topological spaces.*

Solution.

1. We verify the group action axioms. Let $G = \mathbb{C}^\times$ and $X = \mathbb{C}^{n+1}\backslash\{0\}$.
   - Closure: For any $\lambda \in G$ and $\vec{x} = (x_0, \ldots, x_n) \in X$, the product $\lambda \cdot \vec{x} = (\lambda x_0, \ldots, \lambda x_n)$ is a vector in $\mathbb{C}^{n+1}$. Since $\lambda \neq 0$ and $\vec{x} \neq \vec{0}$, at least one component x_i is non-zero, making λx_i non-zero. Thus, $\lambda \cdot \vec{x} \neq \vec{0}$, so the action maps X to itself.

- Identity: The identity element of G is 1. For any $\vec{x} \in X$, $1 \cdot \vec{x} = (1 \cdot x_0, \ldots, 1 \cdot x_n) = \vec{x}$.
- Compatibility: For any $\lambda_1, \lambda_2 \in G$ and $\vec{x} \in X$:

  $(\lambda_1\lambda_2)\cdot\vec{x} = ((\lambda_1\lambda_2)x_0, \ldots, (\lambda_1\lambda_2)x_n) = (\lambda_1(\lambda_2 x_0), \ldots, \lambda_1(\lambda_2 x_n)) = \lambda_1\cdot(\lambda_2\cdot\vec{x})$.

All axioms are satisfied, so this is a well-defined group action.

2. To show $\mathbb{P}^1_{\mathbb{C}}$ is a Riemann surface, we must equip it with an atlas of charts whose transition maps are holomorphic. An element of $\mathbb{P}^1_{\mathbb{C}}$ is an equivalence class $[x_0 : x_1]$ of points in $\mathbb{C}^2\backslash\{0\}$.

   We define two open sets that cover $\mathbb{P}^1_{\mathbb{C}}$:

   - $U_0 = \{[x_0 : x_1] \in \mathbb{P}^1_{\mathbb{C}} \mid x_0 \neq 0\}$.
   - $U_1 = \{[x_0 : x_1] \in \mathbb{P}^1_{\mathbb{C}} \mid x_1 \neq 0\}$.

   These sets are open because their preimages in $\mathbb{C}^2\backslash\{0\}$ are open. They cover $\mathbb{P}^1_{\mathbb{C}}$ because for any point $[x_0 : x_1]$, at least one coordinate must be non-zero.

   We define chart maps for each set:

   - $\phi_0 : U_0 \to \mathbb{C}$ is given by $\phi_0([x_0 : x_1]) = x_1/x_0$. This map is well-defined because if $[x_0 : x_1] = [\lambda x_0 : \lambda x_1]$, then $(\lambda x_1)/(\lambda x_0) = x_1/x_0$. It is a bijection with inverse $\phi_0^{-1}(z) = [1 : z]$.
   - $\phi_1 : U_1 \to \mathbb{C}$ is given by $\phi_1([x_0 : x_1]) = x_0/x_1$. This is also a well-defined bijection, with inverse $\phi_1^{-1}(w) = [w : 1]$.

   The pair (U_0, ϕ_0) and (U_1, ϕ_1) form an atlas. We must check that the transition map is holomorphic. The domain of the transition map is $\phi_0(U_0 \cap U_1)$. $U_0 \cap U_1 = \{[x_0 : x_1] \mid x_0 \neq 0, x_1 \neq 0\}$. The image under ϕ_0 is $\mathbb{C}^\times$.

   The transition map is $\psi = \phi_1 \circ \phi_0^{-1} : \mathbb{C}^\times \to \mathbb{C}^\times$. For any $z \in \mathbb{C}^\times$:

   $$\psi(z) = \phi_1(\phi_0^{-1}(z)) = \phi_1([1 : z]) = \frac{1}{z}.$$

   The function $f(z) = 1/z$ is holomorphic on its domain $\mathbb{C}^\times$. Therefore, the atlas is a complex atlas, endowing $\mathbb{P}^1_{\mathbb{C}}$ with the structure of a Riemann surface. The Hausdorff and second-countable properties are inherited from the quotient topology on $\mathbb{C}^2\backslash\{0\}$.

3. We show that $\mathbb{P}^1_{\mathbb{C}}$ and the 2-sphere S^2 are both homeomorphic to the one-point compactification of $\mathbb{C}$.

   - From part (2), $\mathbb{P}^1_{\mathbb{C}} = U_0 \cup \{[0 : 1]\}$. The chart map $\phi_0 : U_0 \to \mathbb{C}$ is a homeomorphism. So $\mathbb{P}^1_{\mathbb{C}}$ is topologically a copy of $\mathbb{C}$ with a single point, $[0 : 1]$, added. This is the definition of the one-point compactification $\mathbb{C} \cup \{\infty\}$.

- Consider the sphere $S^2 \subset \mathbb{R}^3$. The stereographic projection from the North Pole $(0,0,1)$ is a homeomorphism from $S^2 \backslash \{(0,0,1)\}$ to the plane $\mathbb{R}^2$. Thus, S^2 is topologically the one-point compactification of $\mathbb{R}^2$.

Since $\mathbb{C}$ is homeomorphic to $\mathbb{R}^2$, their one-point compactifications are homeomorphic. Therefore, $\mathbb{P}^1_{\mathbb{C}} \simeq S^2$ as topological spaces.

□

Problem 2.57.

1. *Show that* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \Lambda = \mathbb{Z}(aw_1 + bw_2) \oplus \mathbb{Z}(cw_1 + dw_2)$ *is a well-defined action of* $\mathrm{GL}_2(\mathbb{R})$ *on the space of lattices in* $\mathbb{C}$.
2. *Show that the action* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$ *is a well-defined action of* $\mathrm{GL}_2(\mathbb{R})$ *on* $\mathbb{H}^+ \sqcup \mathbb{H}^-$.
3. *Show that the stabilizer of* $i \in \mathbb{H}^+$ *is* $\mathrm{SO}(2,\mathbb{R}) \cdot \mathbb{R}_{>0}$ *(the group of rotation-dilations) and deduce that* $\mathrm{GL}_2(\mathbb{R})/(\mathrm{SO}(2,\mathbb{R}) \cdot \mathbb{R}_{>0}) \xrightarrow{\sim} \mathbb{H}^+ \sqcup \mathbb{H}^-$.
4. *Show that under this isomorphism, the left action of* $\mathrm{GL}_2(\mathbb{Z})$ *on the coset space corresponds to the standard action on* $\mathbb{H}^+ \sqcup \mathbb{H}^-$.
5. *Show that* $\mathrm{GL}_2(\mathbb{Z}) \backslash (\mathbb{H}^+ \sqcup \mathbb{H}^-) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^+$.

Solution.

1. Let $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ be a lattice. The vectors w_1, w_2 are $\mathbb{R}$-linearly independent. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. Let $w_1' = aw_1 + bw_2$ and $w_2' = cw_1 + dw_2$. If we represent w_1, w_2 as column vectors in $\mathbb{R}^2$ corresponding to their real and imaginary parts, then the new basis vectors (w_1', w_2') are obtained by applying the matrix A to the basis (w_1, w_2). Since A is invertible, it maps an $\mathbb{R}$-basis to another $\mathbb{R}$-basis. Thus, w_1', w_2' are $\mathbb{R}$-linearly independent. The set $A \cdot \Lambda = \mathbb{Z}w_1' \oplus \mathbb{Z}w_2'$ is a discrete subgroup of $\mathbb{C}$ of rank 2, and hence is a lattice. The identity and compatibility axioms for a group action follow directly from the properties of matrix multiplication on basis vectors.
2. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ and $z \in \mathbb{H}^+ \sqcup \mathbb{H}^-$, so $\mathrm{Im}(z) \neq 0$. We compute

the imaginary part of the image:

$$\begin{aligned}
\mathrm{Im}(A \cdot z) &= \mathrm{Im}\left(\frac{az+b}{cz+d}\right) \\
&= \mathrm{Im}\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) \\
&= \frac{\mathrm{Im}(adz+bc\bar{z})}{|cz+d|^2} \\
&= \frac{\mathrm{Im}(ad(x+iy)+bc(x-iy))}{|cz+d|^2} \\
&= \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2} \\
&= \frac{\det(A)\mathrm{Im}(z)}{|cz+d|^2}.
\end{aligned}$$

Since $\det(A) \neq 0$ and $\mathrm{Im}(z) \neq 0$, the imaginary part of the image is also non-zero. Thus $A \cdot z \in \mathbb{H}^+ \sqcup \mathbb{H}^-$. The action axioms follow from standard properties of Möbius transformations.

3. We seek the subgroup of matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ that fix i.

$$\frac{ai+b}{ci+d} = i \implies ai+b = i(ci+d) = -c+di.$$

Equating the real and imaginary parts of this equation gives $b = -c$ and $a = d$. The matrix must have the form $A = \begin{pmatrix} a & -c \\ c & a \end{pmatrix}$. This is a rotation-dilation matrix. The group of such matrices is isomorphic to $\mathbb{C}^\times$ via the map $a + ic \mapsto A$. We can write $A = \sqrt{a^2+c^2}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ where $\cos\theta = a/\sqrt{a^2+c^2}$, etc. This group is precisely the group of scalar multiples of rotation matrices, which we denote $\mathrm{SO}(2,\mathbb{R}) \cdot \mathbb{R}_{>0}$. This is the correct stabilizer, not $O(2,\mathbb{R})$.

The action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{H}^+ \sqcup \mathbb{H}^-$ is transitive. For any $z = x + iy \in \mathbb{H}^+$, the matrix $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ maps i to z. Any point in $\mathbb{H}^-$ can be reached by composing with a matrix of negative determinant, e.g., $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. By the Orbit-Stabilizer Theorem, the orbit of i, which is $\mathbb{H}^+ \sqcup \mathbb{H}^-$, is bijective with the quotient space $G/\mathrm{Stab}_G(i)$. Thus, we have the bijection:

$$\mathrm{GL}_2(\mathbb{R})/(\mathrm{SO}(2,\mathbb{R}) \cdot \mathbb{R}_{>0}) \xrightarrow{\sim} \mathbb{H}^+ \sqcup \mathbb{H}^-.$$

4. The isomorphism $\Psi : \mathrm{GL}_2(\mathbb{R})/\mathrm{Stab}(i) \to \mathbb{H}^+ \sqcup \mathbb{H}^-$ is given by $\Psi(A \cdot \mathrm{Stab}(i)) = A \cdot i$. Let $g \in \mathrm{GL}_2(\mathbb{Z})$ act on the left of the coset space. The

image of the new coset is:

$$\Psi(g \cdot (A \cdot \mathrm{Stab}(i))) = \Psi((gA) \cdot \mathrm{Stab}(i)) = (gA) \cdot i.$$

By the associativity of the Möbius action, this is $g \cdot (A \cdot i)$. If we let $z = A \cdot i$, then the action on the coset space corresponds to the action $z \mapsto g \cdot z$ on the upper half-plane.

5. We want to show $\mathrm{GL}_2(\mathbb{Z})\backslash(\mathbb{H}^+ \sqcup \mathbb{H}^-) \cong \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^+$. Let $\pi : \mathbb{H}^+ \to \mathrm{GL}_2(\mathbb{Z})\backslash(\mathbb{H}^+ \sqcup \mathbb{H}^-)$ be the quotient map restricted to $\mathbb{H}^+$. This map is surjective. For any point $w \in \mathbb{H}^-$, there exists $A \in \mathrm{GL}_2(\mathbb{Z})$ with $\det A = -1$ (e.g., $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) such that $A \cdot w \in \mathbb{H}^+$. Thus, every orbit in the quotient space has a representative in $\mathbb{H}^+$.

   Now we determine the fibers of π. Two points $z_1, z_2 \in \mathbb{H}^+$ map to the same orbit if and only if there exists $g \in \mathrm{GL}_2(\mathbb{Z})$ such that $g \cdot z_1 = z_2$. Since both z_1, z_2 are in $\mathbb{H}^+$, the sign of their imaginary parts is positive. From the formula $\mathrm{Im}(g \cdot z_1) = \frac{\det(g)\mathrm{Im}(z_1)}{|cz_1+d|^2}$, the sign is preserved only if $\det(g) > 0$. Since $g \in \mathrm{GL}_2(\mathbb{Z})$, its determinant must be ± 1. Thus, we must have $\det(g) = 1$, which means $g \in \mathrm{SL}_2(\mathbb{Z})$.

   This shows that two points in $\mathbb{H}^+$ belong to the same $\mathrm{GL}_2(\mathbb{Z})$-orbit if and only if they belong to the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. The quotient space is therefore in bijection with the set of orbits of $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}^+$.

□

3 Wednesday, June 4

3.1 AM Session 1: Trees

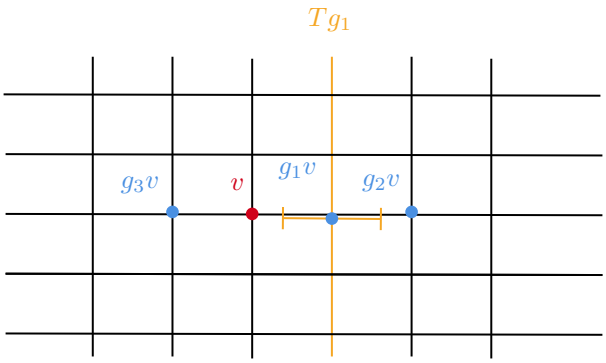
Recall that a group presentation is written as $G \cong \langle S \mid R \rangle$, which signifies that G is isomorphic to the quotient group $F(S)/\langle\langle R \rangle\rangle$. Here, $F(S)$ denotes the free group generated by the set of symbols S, and $\langle\langle R \rangle\rangle$ is the normal closure of the set of relators R (i.e., the smallest normal subgroup containing R). We finished the previous session with the following theorem:

Theorem 3.1. *A group G is free if and only if it acts freely on a tree.*

Proof.

($\implies$). This direction is true by construction. For instance, if $G = F(X)$ is a free group on a set of generators X, its Cayley graph with respect to X is a tree, and G acts freely on this tree by left multiplication.

($\impliedby$). Suppose $G \curvearrowright T$ freely, where T is a tree.



Fix a base vertex $v \in V(T)$. For each $g \in G$, consider the set

$$T_g = \{x \in V(T') \mid d(x, gv) \leqslant d(x, h'v) \text{ for all } h' \in G\}.$$

Here T' denotes the barycentric subdivision of T, and $V(T')$ is its vertex set. The set T_g consists of vertices in T' that are metrically closer to (or equidistant from) gv than to $h'v$ for any other $h' \in G$. T_g induces a subgraph of T'.

Claim:

1. Each $T_g \subseteq T'$ is a connected subgraph (and therefore a subtree, as T' is a tree) and $\bigcup_{g \in G} V(T_g) = V(T')$.
2. If $g \neq h$, then $T_g \cap T_h$ (the intersection of their vertex sets) is either empty or consists of a single vertex.
3. For any $k \in G$, $k \cdot T_h = T_{kh}$ (acting on the vertices and edges of the subgraph).

Let $S = \{g \in G \mid T_{\mathrm{id}} \cap T_g \neq \varnothing\}$, where id is the identity element of G. (Note that $\mathrm{id} \in S$ by this definition, as $T_{\mathrm{id}} \cap T_{\mathrm{id}} = T_{\mathrm{id}}$ is non-empty.)

Exercise 3.2. *If $s \in S$, then $s^{-1} \in S$.*

Claim: $G \cong F(S')$ where $S' = S \backslash \{\mathrm{id}\}$.

Step 1: S generates G.

Take any $g \in G$. Consider the unique simple path in T from v to gv. This path corresponds to a sequence of vertices $v = x_0, x_1, \ldots, x_p = gv$ in T'. Each x_i belongs to some T_k. More formally, there's a sequence $g_0 = \mathrm{id}, g_1, \ldots, g_n = g$ such that $T_{g_k} \cap T_{g_{k+1}} \neq \varnothing$ for $k = 0, \ldots, n-1$. Let $s_k = g_k^{-1} g_{k+1}$. Since $T_{g_k} \cap T_{g_{k+1}} \neq \varnothing$, applying the action of g_k^{-1} yields $g_k^{-1}(T_{g_k} \cap T_{g_{k+1}}) = T_{g_k^{-1} g_k} \cap T_{g_k^{-1} g_{k+1}} = T_{\mathrm{id}} \cap T_{s_k} \neq \varnothing$. Thus, $s_k \in S$ for all k. Then $g_1 = g_0 s_0 = \mathrm{id} \cdot s_0 = s_0$, $g_2 = g_1 s_1 = s_0 s_1$, and so on, leading to $g = g_n = s_0 s_1 s_2 \ldots s_{n-1}$. Thus, S generates G.

Step 2: Why does S freely generate G (when restricted to $S' = S \backslash \{\mathrm{id}\}$)?

Exercise 3.3. *If there were two distinct ways of writing g as a product of elements of S (more precisely, as reduced words in $S' \cup (S')^{-1}$), then this would give a non-trivial loop in T, contradicting that T is a tree.*

This completes the sketch of the proof.

□

Definition 3.4. *The **Farey graph** has:*

- *vertices: pairs $\pm(m, n)$ where $m, n \in \mathbb{Z}$ satisfy $\gcd(|m|, |n|) = 1$. (These represent rational numbers m/n, including ∞ as $\pm(1, 0)$, with (m, n) identified with $(-m, -n)$.)*
- *edges: there is an edge between $\pm(a, b)$ and $\pm(c, d)$ if and only if $ad - bc = \pm 1$.*

Exercise 3.5.

1. *Check that $\pm(0, 1)$ is adjacent to $\pm(1, 0)$.*
2. *Find all vertices $\pm(m, n)$ adjacent to both $\pm(1, 0)$ and $\pm(0, 1)$.*
3. *If $\pm(a, b)$ is adjacent to $\pm(c, d)$, find all vertices $\pm(m, n)$ adjacent to both $\pm(a, b)$ and $\pm(c, d)$. Hint: $SL_2(\mathbb{Z})$ acts on these vertices. The action can be written as $A \cdot \pm(m, n) = \pm \left(A \begin{pmatrix} m \\ n \end{pmatrix} \right)^T$, where the resulting column vector is interpreted as a pair.*

Solution.

1. For $\pm(0,1)$ and $\pm(1,0)$: let $(a,b) = (0,1)$ and $(c,d) = (1,0)$. Then $ad - bc = (0)(0) - (1)(1) = -1$. Since this is ± 1, they are adjacent.
2. Let $\pm(m,n)$ be adjacent to $\pm(1,0)$ and $\pm(0,1)$. Adjacency to $\pm(1,0)$ means $m(0) - n(1) = \pm 1 \implies -n = \pm 1 \implies n = \pm 1$. Adjacency to $\pm(0,1)$ means $m(1) - n(0) = \pm 1 \implies m = \pm 1$. So, the pairs are $(m,n) = (\pm 1, \pm 1)$, with $\gcd(|m|,|n|) = 1$. These are $\pm(1,1)$ and $\pm(1,-1)$.
3. $\pm(a+c, b+d)$ and $\pm(a-c, b-d)$.

□

3.2 AM Session 2: Farey Graphs

To visualize the Farey graph in the upper half-plane $\mathbb{H}$, we identify the vertices $\pm(m,n)$ (where $n \neq 0$) with the rational points $\frac{m}{n}$ on the real axis $\mathbb{R}$. The vertex $\pm(1,0)$ is identified with infinity. The edges of the Farey graph (where $ad - bc = \pm 1$) are then drawn as geodesics in $\mathbb{H}$, which are semicircles perpendicular to $\mathbb{R}$ or vertical lines to ∞. This forms the following picture:

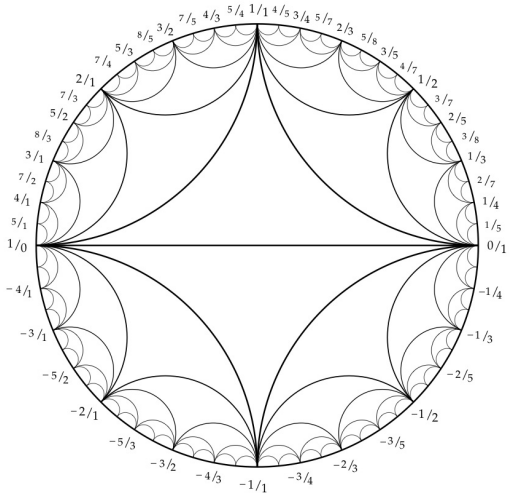


Figure 1: An example of a Farey diagram

From this Farey graph, we construct a tree, denoted T_{far}. The vertices of T_{far} can be conceived as two types: one type representing the centers of the ideal triangles of the Farey tessellation, and the other type representing the midpoints of the edges of the Farey tessellation. An edge in T_{far} connects a vertex representing a triangle-center to a vertex representing an edge-midpoint if the original edge is a boundary of the original triangle.

Exercise 3.6. *Show that T_{far} as described is a tree.*

The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ (preserving the Farey tessellation) induces an action on the constructed tree T_{far}.

Consider the vertex of T_{far} corresponding to the points $\pm(1,0)$ and $\pm(0,1)$. If a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ fixes this vertex, then its columns must be $\pm\begin{pmatrix}1\\0\end{pmatrix}$ and $\pm\begin{pmatrix}0\\1\end{pmatrix}$, in some order. The only such matrices in $\mathrm{SL}_2(\mathbb{Z})$ are:

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&-1\\1&0\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\} \cong \mathbb{Z}/4\mathbb{Z}.$$

Similarly, consider the center of the Farey graph, which corresponds to the points $\pm(1,0)$, $\pm(0,1)$, and $\pm(1,1)$. If $A \in \mathrm{SL}_2(\mathbb{Z})$ fixes all of these, then its columns must be some pair of these vectors (up to sign) that form a basis. The only possibilities are:

$$\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\-1&1\end{pmatrix}, \begin{pmatrix}1&-1\\1&0\end{pmatrix}\right\} \cong \mathbb{Z}/6\mathbb{Z}.$$

Since the subgroup $\{\pm I\} \subseteq \mathrm{SL}_2(\mathbb{Z})$ (where I is the identity matrix) acts trivially on T_{far} (as $\pm(m,n)$ is identified with $\mp(m,n)$ as vertices of the original Farey graph), the action descends to an action of

$$\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}.$$

The stabilizers of the above types of vertices in T_{far} under the $\mathrm{PSL}_2(\mathbb{Z})$ action become $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, respectively.

Note: The action of $\mathrm{PSL}_2(\mathbb{Z})$ on T_{far} has trivial edge stabilizers. That is, if an element of $\mathrm{PSL}_2(\mathbb{Z})$ fixes an edge of T_{far}, it must be the identity element in $\mathrm{PSL}_2(\mathbb{Z})$.

Definition 3.7. *The **free product** of groups G and H, denoted $G * H$, is the group whose elements are finite sequences (words) of the form $x_1 x_2 \dots x_k$ where each x_i is a non-identity element of either G or H, and adjacent elements x_j, x_{j+1} belong to different groups. The identity element is represented by the empty word. The group operation is concatenation of words followed by reduction (e.g., if $g_1, g_2 \in G$, $g_1 g_2$ within a word is replaced by their product in G; if this product is e_G, it is removed, potentially leading to further reductions).*

Exercise 3.8. *If $G \cong \langle S_G \mid R_G \rangle$ and $H \cong \langle S_H \mid R_H \rangle$ (assuming S_G and S_H are disjoint), then*

$$G * H \cong \langle S_G \cup S_H \mid R_G \cup R_H \rangle.$$

Example 3.9. *Let $G = \mathbb{Z}/2\mathbb{Z} = \langle a \mid a^2 = e \rangle$ and $H = \mathbb{Z}/2\mathbb{Z} = \langle b \mid b^2 = e \rangle$. Then $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z} \cong \langle a, b \mid a^2, b^2 \rangle$. Elements are alternating strings of a's and b's, such as ababab, ababa, a, b, and the empty word (identity). This group is the infinite dihedral group D_∞.*

Theorem 3.10. *Suppose a group G acts on a tree T satisfying:*

1. *The action is without inversions (if an element $g \in G$ fixes an edge $e = (u, v)$, then $gu = u$ and $gv = v$).*
2. *The action is transitive on the set of oriented edges of T.*
3. *The stabilizer G_e of an edge e is trivial.*

Fix an edge $e = (v_1, v_2)$ in T. Let $H_1 = G_{v_1}$ and $H_2 = G_{v_2}$ be the stabilizers of its vertices. Then $G \cong H_1 * H_2$.

Proof. The key idea is to describe elements of G in terms of elements from H_1 and H_2, using paths in the tree T on which G acts.

Step 1: Show that G is generated by $H_1 \cup H_2$.

Let $g \in G$. Consider the tree T, and let v be a vertex stabilized by H_1. Then the vertex gv is stabilized by the conjugate subgroup gH_1g^{-1}. Since the tree is connected, there is a path from v to gv. This path corresponds to a sequence of adjacent vertices:

$$v = v_0, v_1, \ldots, v_n = gv,$$

where each pair (v_i, v_{i+1}) is connected by an edge. The stabilizer of each edge lies in either H_1 or H_2, depending on which edge of the tree it is associated with.

Let $g_i \in G$ be such that $g_i v = v_i$, for $i = 0, \ldots, n$, with $g_0 = 1$ and $g_n = g$. Then for each i, the element $g_i^{-1} g_{i+1}$ stabilizes the edge between v_i and v_{i+1}, so $g_i^{-1} g_{i+1} \in H_1 \cup H_2$. Thus we can write:

$$g = g_n = (g_0^{-1} g_1)(g_1^{-1} g_2) \cdots (g_{n-1}^{-1} g_n),$$

where each factor lies in either H_1 or H_2. This shows that G is generated by $H_1 \cup H_2$.

Step 2: Show uniqueness of such expressions.

Suppose $g \in G$ has an expression as a product of elements from H_1 and H_2 alternating in a reduced form (i.e., no consecutive elements from the same subgroup and no identity elements). Then this corresponds to a reduced path in the tree T, and such a path is unique because T is a tree (i.e., it has no cycles). Hence the decomposition of g into such a product is unique up to the rules of the amalgamated product.

This completes the proof. □

Corollary 3.11.

$$PSL_2(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}.$$

Consequently, a presentation for $PSL_2(\mathbb{Z})$ is

$$PSL_2(\mathbb{Z}) \cong \langle a, b \mid a^2 = e, b^3 = e \rangle.$$

Proof. We apply the previous theorem. All that's left is to check that $\mathrm{PSL}_2(\mathbb{Z})$ acts transitively on edges of T_{far}. □

3.3 AM Problem Session

Problem 3.12. *Prove the following facts about a group action $G \curvearrowright X$:*

1. *For each $x \in X$ and $g \in G$, the stabilizer satisfies $G_{gx} = gG_xg^{-1}$.*
2. *If a normal subgroup $H \trianglelefteq G$ acts trivially on X, then there is a well-defined action $G/H \curvearrowright X$ by $(gH) \cdot x = g \cdot x$.*

Solution.

1. To establish the equality of the sets G_{gx} and gG_xg^{-1}, we demonstrate mutual inclusion.

   First, let $h \in G_{gx}$. By definition, $h \cdot (gx) = gx$. The axioms of a group action permit rewriting this as $(hg) \cdot x = gx$. Applying the action of g^{-1} from the left yields $g^{-1} \cdot ((hg) \cdot x) = g^{-1} \cdot (gx)$, which simplifies to $(g^{-1}hg) \cdot x = x$. This shows that the element $g^{-1}hg$ is in the stabilizer G_x. Consequently, $h = g(g^{-1}hg)g^{-1}$, which proves that h is an element of gG_xg^{-1}. Thus, $G_{gx} \subseteq gG_xg^{-1}$.

   Conversely, let $h \in gG_xg^{-1}$. Then h can be expressed as $h = gkg^{-1}$ for some $k \in G_x$, where $k \cdot x = x$. We verify that h stabilizes the element gx:

   $$h \cdot (gx) = (gkg^{-1}) \cdot (gx) = (gkg^{-1}g) \cdot x = (gk) \cdot x = g \cdot (k \cdot x) = g \cdot x.$$

   This confirms that $h \in G_{gx}$, thereby establishing the inclusion $gG_xg^{-1} \subseteq G_{gx}$. The two inclusions together imply the desired equality.

2. For the action of the quotient group G/H to be well-defined, the result must be independent of the choice of coset representative. Let $g_1, g_2 \in G$ be such that $g_1H = g_2H$. This equivalence implies that $g_2 = g_1h$ for some $h \in H$. We must show that the action of the coset, when computed using either representative, yields the same result. We compute the action of g_2 on an element $x \in X$:

   $$g_2 \cdot x = (g_1h) \cdot x = g_1 \cdot (h \cdot x).$$

   By hypothesis, the normal subgroup H acts trivially on X, meaning $h \cdot x = x$ for all $h \in H$. Substituting this into the previous equation gives:

   $$g_1 \cdot (h \cdot x) = g_1 \cdot x.$$

   Thus, $g_2 \cdot x = g_1 \cdot x$, confirming that the action is well-defined. The verification that this well-defined operation satisfies the group action axioms for G/H is a straightforward consequence of the fact that the original operation for G is a group action.

□

Problem 3.13. *Given a free action of a group on a tree, verify that the standard construction of a fundamental domain yields a valid tiling of the tree.*

Solution. Let G act freely on a tree T. The objective is to construct a fundamental domain, a subtree whose translates under the action of G partition T. The canonical method involves the quotient graph $\Gamma = G\backslash T$, whose vertices and edges are the orbits of those of T. Since the action is free, the natural projection $p : T \to \Gamma$ is a covering map. The construction begins by selecting a maximal tree $T_0 \subseteq \Gamma$. By the lifting property for covering spaces, we can lift T_0 to a subtree $\tilde{T}_0 \subset T$. This lift, our fundamental domain, is unique up to the choice of a base vertex.

We verify that the set of translates $\{g\tilde{T}_0 \mid g \in G\}$ forms a partition of T. First, we show the union of translates covers T. Let $v \in V(T)$ be an arbitrary vertex. Its orbit, Gv, must contain a vertex v' whose projection $p(v')$ lies in the maximal tree T_0. Since the projection p restricted to the lift $\tilde{T}_0$ is a bijection onto T_0, there is a unique vertex $\tilde{v} \in \tilde{T}_0$ such that $p(\tilde{v}) = p(v')$. Because v' and $\tilde{v}$ lie in the same orbit and project to the same point, there exists some $g \in G$ such that $v' = g\tilde{v}$. As v and v' are also in the same orbit, there exists $h \in G$ such that $v = hv'$. Combining these, we find $v = hg\tilde{v}$, which implies v belongs to the translate $(hg)\tilde{T}_0$. A similar argument holds for edges.

Next, we show the interiors of these tiles are disjoint. Suppose $v \in \tilde{T}_0 \cap g\tilde{T}_0$ for some $g \neq e$. This implies $v \in \tilde{T}_0$ and $v = gv'$ for some $v' \in \tilde{T}_0$. Applying the projection map gives $p(v) = p(gv') = p(v')$. Since the restriction $p|_{\tilde{T}_0} : \tilde{T}_0 \to T_0$ is an isomorphism of graphs, it is injective on vertices. Therefore, $p(v) = p(v')$ implies $v = v'$. The condition becomes $v = gv$. As the action of G on T is free, this forces $g = e$, which contradicts our assumption. Thus, for any $g \neq e$, the intersection $\tilde{T}_0 \cap g\tilde{T}_0$ contains no vertices. The construction thus partitions the vertices and edges of the tree. □

Problem 3.14. *Consider the principal congruence subgroup*

$$\Gamma(m) = \ker(\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})).$$

Show that if $m \geqslant 3$, then $\Gamma(m)$ is a free group.

Solution. The proof relies on the relationship between a group and the topology of its quotient space when it acts on a suitable space. The modular group $\mathrm{SL}(2,\mathbb{Z})$ acts on the complex upper half-plane $\mathbb{H}$, but this action is not free due to the presence of elliptic elements of finite order, which have fixed points. The core of the argument is to show that for $m \geqslant 3$, the subgroup $\Gamma(m)$ is torsion-free, and therefore acts freely on $\mathbb{H}$.

An element of $\mathrm{SL}(2,\mathbb{Z})$ has finite order if and only if it is conjugate to a power of $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (order 4) or $T = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ (order 6), or is $-I$ (order 2). We check if any of these lie in $\Gamma(m)$ by applying the reduction homomorphism $\pi_m : \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/m\mathbb{Z})$. An element is in the kernel $\Gamma(m)$ if it maps to the identity. The matrices S and T do not reduce to the identity modulo m for any $m > 1$. The matrix $-I$ reduces to the identity if and only if $-1 \equiv 1 \pmod{m}$, which means m divides 2. Therefore, for $m \geqslant 3$, none of the elliptic elements of $\mathrm{SL}(2,\mathbb{Z})$ lie in $\Gamma(m)$, proving that $\Gamma(m)$ is torsion-free.

Since $\Gamma(m)$ is a torsion-free discrete subgroup of $\mathrm{SL}(2,\mathbb{Z})$, its action on $\mathbb{H}$ is free. The quotient space $X(m) = \Gamma(m)\backslash\mathbb{H}$ is a Riemann surface, and the projection $\mathbb{H} \to X(m)$ is a covering map. As $\mathbb{H}$ is contractible, it is the universal cover of $X(m)$. The theory of covering spaces provides an isomorphism between the group of deck transformations, which is $\Gamma(m)$, and the fundamental group of the base space, $\pi_1(X(m))$.

Topologically, the surface $X(m)$ is a sphere with a finite number of punctures (the cusps). For $m \geqslant 3$, the number of punctures is at least three. A sphere with $k \geqslant 2$ punctures is homotopy equivalent to a wedge of $k-1$ circles, whose fundamental group is the free group on $k-1$ generators, F_{k-1}. Therefore, for $m \geqslant 3$, $\Gamma(m)$ is isomorphic to a non-trivial free group. □

Problem 3.15.

1. *Prove that a free product of two groups acts on a tree without inversions, freely and transitively on edges.*
2. *Prove that a free product with amalgamation acts on a tree without inversions and transitively on edges.*

Solution. This problem describes the construction of the Bass-Serre tree for a free product, both with and without amalgamation.

First, consider the free product $G = A * B$. We construct a bipartite graph T whose vertex set is the disjoint union of the left cosets of the factor groups, $V(T) = (G/A) \sqcup (G/B)$. The edge set is identified with the group itself, $E(T) = G$, where an edge $g \in G$ connects the vertex gA to the vertex gB. The group G acts on this graph by left multiplication. This graph is a tree; connectivity is straightforward, and the uniqueness of the normal form for elements in a free product ensures the absence of cycles. A cycle would correspond to a non-trivial reduced word being equal to the identity, which is impossible. The action is without inversions, as an element inverting an edge would have to belong to both A and B, but $A \cap B = \{e\}$. The action is transitive on edges by construction, and it is free on edges since the stabilizer of an edge g is trivial. The vertex stabilizers are the conjugates of the non-trivial factor groups A and B.

Next, consider the amalgamated free product $G = A *_C B$, where A and B share a common subgroup C. The construction of the tree is analogous. The vertex set is again $V(T) = (G/A) \sqcup (G/B)$. The edge set, however, is now identified with the left cosets of the amalgamated subgroup, $E(T) = G/C$. An edge corresponding to the coset gC connects the vertex gA to the vertex gB. The action of G is again by left multiplication. The proof that this graph is a tree is a deeper result that relies on the uniqueness of the normal form for elements in an amalgamated product. The action is transitive on edges by construction. It is without inversions, as an element h inverting an edge gC must satisfy $g^{-1}hg \in A$ and $g^{-1}hg \in B$, which implies $g^{-1}hg \in C$. This reveals that the stabilizer of the edge gC is the conjugate subgroup gCg^{-1}. Since C is generally non-trivial, the action on edges is not free. The vertex stabilizers are the conjugate subgroups of A and B.

Brief remark: This construction provides the geometric foundation for Bass-Serre theory. It is a generalization of the Cayley graph, which can be seen as the special case where the factor groups are trivial ($A = B = C = \{e\}$), resulting in the standard Cayley graph of a free group. □

Problem 3.16. *Prove that every automorphism of a tree T is either elliptic or hyperbolic. An elliptic automorphism is a transformation that fixes a vertex or an edge. A hyperbolic automorphism is a transformation g that preserves a bi-infinite path $L \subset T$, called its axis, and acts by translation along L.*

Solution. Let $\phi : T \to T$ be a tree automorphism, which is an isometry under the path metric d. Define the displacement function $\delta(v) = d(v, \phi(v))$ for $v \in V(T)$, and let $\ell = \inf_{v \in V(T)} \delta(v)$ be the minimal displacement. The proof proceeds by analyzing whether this infimum is attained.

First, suppose the minimum is attained, so there exists a vertex v_0 with $\delta(v_0) = \ell$. If $\ell = 0$, then $\phi(v_0) = v_0$, and ϕ is elliptic by definition. If $\ell > 0$, let P be the unique geodesic from v_0 to $\phi(v_0)$. For any point v on P, the displacement $\delta(v)$ is also equal to ℓ, a key property of isometries on CAT(0) spaces like trees. Let m be the midpoint of P. Since ϕ maps the geodesic P to the geodesic $\phi(P)$ (from $\phi(v_0)$ to $\phi^2(v_0)$), and all points on P have minimal displacement, the path $\phi(P)$ must align with P without increasing displacement. This implies the midpoint of P is mapped to the midpoint of $\phi(P)$. In a tree, this forces an overlap. If the length of P is even, m is a vertex and $\phi(m) = m$. If the length is odd, m is the center of an edge e, and $\phi(e) = e$. In either case, ϕ stabilizes a vertex or an edge and is therefore elliptic.

Next, suppose the infimum $\ell > 0$ is not attained. This implies the existence of a bi-infinite geodesic path $L \subset T$, the axis, which is invariant under ϕ. Since ϕ is an isometry, it maps the geodesic L to another geodesic, which must be L itself. Thus, ϕ acts as a permutation on the vertices of L that preserves adjacency and distance. This forces ϕ to act as a translation along L. That is, if L is parameterized by the integers $(\dots, v_{-1}, v_0, v_1, \dots)$, there exists a non-zero

integer n (the translation length) such that $\phi(v_i) = v_{i+n}$ for all $i \in \mathbb{Z}$. Such an automorphism is, by definition, hyperbolic. □

Problem 3.17. *Explain how to give a presentation of a group G acting on a tree T without inversions, transitively on both edges and vertices.*

Solution. This scenario is a fundamental application of Bass-Serre theory, leading to the algebraic structure of an HNN extension. Let G act on a tree T without inversions and with a single orbit of vertices and a single orbit of edges. The quotient graph $G\backslash T$ therefore consists of one vertex and one loop edge.

We derive a presentation by choosing representatives in the tree. Select a vertex $v_0 \in V(T)$ and an edge $e_0 \in E(T)$ whose initial vertex is v_0. Let the terminal vertex of e_0 be v_1. The stabilizer subgroups of these representatives are $A = \mathrm{Stab}_G(v_0)$ and $H_0 = \mathrm{Stab}_G(e_0)$. Since an edge stabilizer fixes the endpoints, $H_0 \subseteq A$.

Because the action is transitive on vertices, there must be an element, which we call the stable letter $t \in G$, that connects the vertices of the representative edge, i.e., $t \cdot v_1 = v_0$. This element relates the stabilizer of v_1 to that of v_0 by conjugation: $G_{v_1} = t^{-1}At$. The stabilizer H_0 is a subgroup of both G_{v_0} and G_{v_1}. From $H_0 \subseteq G_{v_1}$, we conjugate by t to find $tH_0t^{-1} \subseteq tG_{v_1}t^{-1} = G_{tv_1} = G_{v_0} = A$. Thus, conjugation by t defines an injective homomorphism $\psi : H_0 \to A$ given by $\psi(h) = tht^{-1}$. Let $H_1 = \psi(H_0) \subseteq A$.

The structure theorem of Bass-Serre theory asserts that G is generated by the vertex stabilizer group A and the stable letter t. The interaction between these generators is completely described by the isomorphism between the subgroups H_0 and H_1. This gives the presentation for the **Higgman-Neumann-Neumann (HNN) extension**:

$$G \cong \langle A, t \mid tht^{-1} = \psi(h) \text{ for all } h \in H_0 \rangle$$

In this notation, A represents the full presentation (generators and relations) of the vertex stabilizer group. □

Problem 3.18. *Consider the Baumslag-Solitar groups, $BS(m, n) = \langle a, b \mid ba^mb^{-1} = a^n \rangle$. Show that this group acts on a tree and relate this to the HNN extension structure.*

Solution. The Baumslag-Solitar group $\mathrm{BS}(m, n)$ is a canonical example of an HNN extension. We can directly identify its components from the presentation. The base group is $A = \langle a \rangle \cong \mathbb{Z}$. The stable letter is $t = b$. The defining relation $ba^mb^{-1} = a^n$ provides the isomorphism ψ between two subgroups of A: the domain is $H_0 = \langle a^m \rangle \cong \mathbb{Z}$, and the codomain is $H_1 = \langle a^n \rangle \cong \mathbb{Z}$. The isomorphism is explicitly given by $\psi(a^m) = a^n$.

Since $\mathrm{BS}(m,n)$ is an HNN extension, Bass-Serre theory guarantees it acts on its Bass-Serre tree $T_{m,n}$. This tree can be constructed explicitly with vertices corresponding to the left cosets of the base group, $V(T_{m,n}) = \{gA \mid g \in \mathrm{BS}(m,n)\}$, and edges corresponding to the left cosets of the associated subgroup, $E(T_{m,n}) = \{gH_0 \mid g \in \mathrm{BS}(m,n)\}$. An edge gH_0 connects the vertex gA to the vertex gbA.

The action of $\mathrm{BS}(m,n)$ on this tree is by left multiplication. The stabilizer of a vertex gA is the conjugate subgroup $gAg^{-1} \cong \mathbb{Z}$. The stabilizer of an edge gH_0 is the conjugate subgroup $gH_0g^{-1} \cong \mathbb{Z}$. The action is transitive on both vertices and edges by construction. Geometrically, the tree is an $(m+n)$-regular tree where vertices can be imagined as arranged in levels. The generator a acts as a translation along a given level, while the generator b acts as a shift between levels, connecting a block of m vertices from one level to a block of n on another, encapsulating the relation. □

Problem 3.19. *Show that BS*$(2,3) = \langle a, b \,|\, ba^2b^{-1} = a^3 \rangle$ *is non-Hopfian.*

Solution. A group G is Hopfian if every surjective endomorphism $\phi : G \to G$ is an isomorphism. To prove that $\mathrm{BS}(2,3)$ is non-Hopfian, we must construct a surjective endomorphism that possesses a non-trivial kernel.

Define the endomorphism $\phi : \mathrm{BS}(2,3) \to \mathrm{BS}(2,3)$ on the generators by $\phi(a) = a^2$ and $\phi(b) = b$. We verify this is a valid homomorphism by checking that the images satisfy the group's defining relation. The image of the left side of the relation is $\phi(b)\phi(a)^2\phi(b)^{-1} = b(a^2)^2b^{-1} = ba^4b^{-1} = (ba^2b^{-1})^2 = (a^3)^2 = a^6$. The image of the right-hand side is $\phi(a)^3 = (a^2)^3 = a^6$. Since the images satisfy the relation, ϕ is a well-defined endomorphism.

Next, we establish that ϕ is surjective. The image of ϕ is the subgroup generated by the images of the generators, $\mathrm{Im}(\phi) = \langle a^2, b \rangle$. Since b and a^2 are in the image, the element $ba^2b^{-1} = a^3$ must also be in the image. As the image subgroup contains both a^2 and a^3, and because $\gcd(2,3) = 1$, it must also contain $a = a^{1\cdot 3 - 1\cdot 2} = a^3(a^2)^{-1}$. Because both generators a and b are in the image, the endomorphism is surjective.

Finally, we must demonstrate that the kernel of ϕ is non-trivial. This requires the machinery of HNN extensions, specifically Britton's Lemma, which gives a normal form for elements and a criterion for triviality. Consider the element $w = [a, bab^{-1}] = a(bab^{-1})a^{-1}(bab^{-1})^{-1}$. We compute its image under ϕ:

$$\phi(w) = [\phi(a), \phi(b)\phi(a)\phi(b)^{-1}] = [a^2, ba^2b^{-1}].$$

Using the defining relation $ba^2b^{-1} = a^3$, this becomes:

$$\phi(w) = [a^2, a^3].$$

Since a^2 and a^3 are powers of the same element, they commute. Therefore, their commutator is the identity: $\phi(w) = e$. This shows that w is in the kernel of ϕ.

The proof is complete if we show that w is a non-trivial element of $\mathrm{BS}(2,3)$. This is the most technical step. Britton's Lemma states that if a word in an HNN extension equals the identity, it must contain a "pinch" subword of the form tct^{-1} where c is in the first associated subgroup, or $t^{-1}ct$ where c is in the second. For $\mathrm{BS}(2,3)$, this means any trivial word must contain a subword of the form $ba^{2k}b^{-1}$ or $b^{-1}a^{3k}b$ for some non-zero integer k. The word $w = abab^{-1}a^{-1}bab^{-1}$ does not contain such a subword and cannot be reduced to one. We've handwaved this mostly, but a rigorous application of Britton's Lemma confirms that $w \neq e$.

Since we have constructed a surjective endomorphism ϕ with a non-trivial kernel, $\mathrm{BS}(2,3)$ is non-Hopfian. □

3.4 PM Session 1: Moduli I

Let $\Gamma(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ be the principal congruence subgroup of level $N \geqslant 2$, defined as the set of matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that $a, d \equiv 1 \pmod{N}$ and $b, c \equiv 0 \pmod{N}$. The action of $\Gamma(N)$ on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ by fractional linear transformations gives rise to the modular curve $Y(N) := \Gamma(N)\backslash\mathbb{H}$. These are non-compact Riemann surfaces.

In the special case where $N = 1$, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. The corresponding modular curve $Y(1)$ is isomorphic to the complex plane via the j-invariant:

$$\begin{aligned} Y(1) &\xrightarrow{\sim} \mathbb{C} \\ z &\mapsto j(z) \end{aligned}$$

To work with a compact space, we can compactify $Y(N)$ to obtain a compact Riemann surface denoted by $X(N)$. This is achieved by adding a finite number of points called "cusps," resulting in a smooth projective curve with an embedding $Y(N) \hookrightarrow X(N)$.

Every point of $Y(1)$ corresponds to a homothety class of lattices $\Lambda \subseteq \mathbb{C}$. Each such lattice defines an elliptic curve $E = \mathbb{C}/\Lambda$. This elliptic curve can be embedded into the complex projective plane $\mathbb{P}^2$ via the Weierstrass $\wp$-function and its derivative:

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\sim} Z(Y^2Z - 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3) \subseteq \mathbb{P}^2 \\ t &\mapsto [\wp_\Lambda(t) : \wp'_\Lambda(t) : 1] \\ 0 &\mapsto [0 : 1 : 0] \end{aligned}$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ are defined in terms of the Eisenstein series $G_{2k}(\Lambda) = \sum_{w \in \Lambda \setminus \{0\}} w^{-2k}$.

The coefficients g_2 and g_3 transform under scaling of the lattice Λ by $\alpha \in \mathbb{C}^\times$ as follows: $g_2(\alpha\Lambda) = \alpha^{-4} g_2(\Lambda)$ and $g_3(\alpha\Lambda) = \alpha^{-6} g_3(\Lambda)$. The j-invariant, defined as

$$j(\Lambda) = \frac{1728 g_2(\Lambda)^3}{\Delta(\Lambda)} \quad \text{where} \quad \Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2,$$

is invariant under such scaling (i.e., it is of weight 0), and thus depends only on the homothety class of the lattice.

Definition 3.20. *Let $f : \mathbb{H} \to \mathbb{C}$ be a holomorphic function. We say that f is a **modular form of weight** $2k$ **and level** N if:*

1. *For every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$, $f(\gamma z) = (cz + d)^{2k} f(z)$.*
2. *f is holomorphic at the cusps (i.e., on the boundary $X(N) \backslash Y(N)$).*

Lemma 3.21. *Let $\mathcal{L}$ be the set of all lattices in $\mathbb{C}$, and let $F : \mathcal{L} \to \mathbb{C}$ be a function satisfying the homogeneity condition $F(\alpha\Lambda) = \alpha^{-2k} F(\Lambda)$ for any $\alpha \in \mathbb{C}^\times$. If we define a function $f : \mathbb{H} \to \mathbb{C}$ by setting $f(\tau) = F(\mathbb{Z}\tau \oplus \mathbb{Z})$, then f satisfies the transformation property of a modular form of weight $2k$ for $SL_2(\mathbb{Z})$. If f is also holomorphic on $\mathbb{H}$ and at the cusp, it is a modular form of weight $2k$ and level 1.*

Proof. A lattice Λ with basis (ω_1, ω_2) can be written as $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. The homogeneity condition allows us to view F as a function of the basis, where $F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k} F(\omega_1, \omega_2)$. By setting $\lambda = \omega_2^{-1}$ and $\tau = \omega_1/\omega_2 \in \mathbb{H}$, we can write:

$$F(\omega_1, \omega_2) = \omega_2^{-2k} F(\tau, 1) = \omega_2^{-2k} f(\tau)$$

Now, consider a change of basis given by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. The new basis is $(\omega_1', \omega_2') = (a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$, which generates the same lattice. The new ratio is $\tau' = \frac{\omega_1'}{\omega_2'} = \frac{a\tau + b}{c\tau + d}$. Since the lattice is unchanged, $F(\omega_1', \omega_2') = F(\omega_1, \omega_2)$. Using our relation, we have:

$$\begin{aligned}
F(\omega_1, \omega_2) &= F(\omega_1', \omega_2') \\
\omega_2^{-2k} f(\tau) &= (\omega_2')^{-2k} f(\tau') \\
\omega_2^{-2k} f(\tau) &= (c\omega_1 + d\omega_2)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right) \\
\omega_2^{-2k} f(\tau) &= \omega_2^{-2k} (c\tau + d)^{-2k} f\left(\frac{a\tau + b}{c\tau + d}\right)
\end{aligned}$$

Canceling the ω_2^{-2k} term yields the desired modular transformation property:

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{2k} f(\tau)$$

□

Corollary 3.22. *The functions g_2 (derived from G_4) and g_3 (derived from G_6) correspond to modular forms of weight 4 and 6 respectively, for level 1. The discriminant function $\Delta = g_2^3 - 27g_3^2$ corresponds to a modular form of weight 12 and level 1.*

The set of modular forms of a fixed weight $2k$ and level N forms a finite-dimensional $\mathbb{C}$-vector space, which we denote by $M_{2k}(N)$. The product of a form $f \in M_{2k}(N)$ and a form $g \in M_{2\ell}(N)$ is a modular form $f \cdot g \in M_{2(k+\ell)}(N)$. Consequently, the direct sum over all non-negative weights forms a graded, commutative $\mathbb{C}$-algebra:

$$\bigoplus_{k \geqslant 0} M_{2k}(N)$$

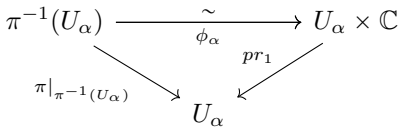
The concept of a modular form can be rephrased in the geometric language of line bundles. To introduce this, we first recall the relationship between functions and sections of a trivial bundle.

Let X be a Riemann surface. The **trivial line bundle** over X is the product space $L = X \times \mathbb{C}$, equipped with the standard projection map $p_1 : X \times \mathbb{C} \to X$ onto the first factor.

Theorem 3.23. *A holomorphic function on X is equivalent to a holomorphic section of the trivial line bundle. A section is a holomorphic map $s : X \to X \times \mathbb{C}$ such that $p_1(s(x)) = x$ for all $x \in X$. Any such section is of the form $s(x) = (x, f(x))$ for some holomorphic function $f : X \to \mathbb{C}$.*

3.5 PM Session 2: Moduli II

Definition 3.24. *A **line bundle** over a complex manifold X is a complex manifold L together with a surjective holomorphic map $\pi : L \to X$ satisfying the following condition: there exists an open cover $\{U_\alpha\}$ of X and biholomorphisms $\phi_\alpha : \pi^{-1}(U_\alpha) \to U_\alpha \times \mathbb{C}$ such that the following diagram commutes:*



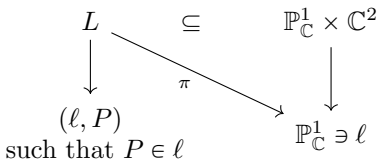
Here, pr_1 is the standard projection onto the first factor. For each point $x \in U_\alpha$, the restriction of ϕ_α to the fiber $\pi^{-1}(x)$ is a $\mathbb{C}$-linear isomorphism onto $\{x\} \times \mathbb{C} \cong \mathbb{C}$.

Recall that the complex projective line $\mathbb{P}^1_{\mathbb{C}}$ is the space of lines through the origin in $\mathbb{C}^2$. It can be constructed as the quotient space $(\mathbb{C}^2 \backslash \{0\})/\mathbb{C}^\times$.

A fundamental example of a line bundle is the **tautological line bundle** over $\mathbb{P}^1_{\mathbb{C}}$. Consider the subset $L \subseteq \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}^2$ defined by

$$L = \{(\ell, P) \in \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}^2 \mid P \in \ell\}.$$

The projection map $\pi : L \to \mathbb{P}^1_{\mathbb{C}}$ is given by $\pi(\ell, P) = \ell$.



For any point $\ell \in \mathbb{P}^1_{\mathbb{C}}$, the fiber $\pi^{-1}(\ell)$ is $\{(\ell, P) \mid P \in \ell\}$, which is canonically isomorphic to the line ℓ itself. This makes L a line bundle over $\mathbb{P}^1_{\mathbb{C}}$.

Now, let H be a Riemann surface with an action of a group Γ such that the quotient space $X = \Gamma\backslash H$ is also a Riemann surface. Let $q : H \to X$ be the quotient map. Given a line bundle $\pi : L \to X$, we can form the **pullback line bundle** q^*L over H. It is defined as the fibered product:

$$q^*L = \{(\tau, v) \in H \times L \mid q(\tau) = \pi(v)\}.$$

$$\begin{array}{ccc} H & \longleftarrow & q^*L = \{(\tau, z) | q(\tau) = \pi(z)\} \\ {\scriptstyle q}\downarrow & & \downarrow \\ X & \xleftarrow[\pi]{} & L \end{array}$$

Lemma 3.25.

1. *The pullback q^*L is a line bundle on H.*
2. *The group Γ acts on q^*L, and the quotient of q^*L by this action is isomorphic to L.*

If H is simply connected (for instance, the upper half-plane $\mathbb{H}$), any line bundle on it is trivial. Thus, we have a biholomorphism $\phi : q^*L \xrightarrow{\sim} H \times \mathbb{C}$.

$$q^*L \xrightarrow[\phi]{\sim} H \times \mathbb{C}$$

The action of Γ on q^*L induces an action on $H \times \mathbb{C}$ via ϕ that is compatible with the action on H. This means that for any $\gamma \in \Gamma$, the action must be of the form:

$$\gamma \cdot (\tau, z) = (\gamma\tau, j_\gamma(\tau)z)$$

for some holomorphic function $j_\gamma : H \to \mathbb{C}^\times$. The group structure of Γ imposes a consistency condition on these functions. For any $\gamma, \gamma' \in \Gamma$, the equality $(\gamma\gamma') \cdot (\tau, z) = \gamma \cdot (\gamma' \cdot (\tau, z))$ implies:

$$j_{\gamma\gamma'}(\tau) = j_\gamma(\gamma'\tau) j_{\gamma'}(\tau). \qquad (\star)$$

Definition 3.26. *A function $j : \Gamma \times H \to \mathbb{C}^\times$, written as $(\gamma, \tau) \mapsto j_\gamma(\tau)$, is a **factor of automorphy** if it is holomorphic in τ for each fixed $\gamma \in \Gamma$ and satisfies the cocycle condition $(\star)$.*

Proposition 3.27.

1. *Every line bundle on $Y(N) = \Gamma(N)\backslash\mathbb{H}$ is uniquely determined, up to isomorphism, by a factor of automorphy $j : \Gamma(N) \times \mathbb{H} \to \mathbb{C}^\times$.*
2. *For an integer k, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. The function $j : \Gamma(N) \times \mathbb{H} \to \mathbb{C}^\times$ defined by $j_\gamma(\tau) = (c\tau + d)^{2k}$ is a factor of automorphy.*
3. *If $\mathcal{L}_{2k}$ is the line bundle corresponding to this factor of automorphy, then modular forms of weight $2k$ for $\Gamma(N)$ are precisely the holomorphic sections of $\mathcal{L}_{2k}$.*

We now shift our perspective to the moduli interpretation of modular curves. The points of the modular curve $Y(1) = \Gamma(1)\backslash\mathbb{H}$ are in one-to-one correspondence with the isomorphism classes of elliptic curves over $\mathbb{C}$. Using the language of algebraic geometry, we can say that the set of $\mathbb{C}$-points of $Y(1)$, denoted $\mathrm{Hom}(\mathrm{Spec}(\mathbb{C}), Y(1))$, parameterizes isomorphism classes of elliptic curves.

What about families of elliptic curves? For an arbitrary complex manifold (or scheme) T, what does a map $T \to Y(1)$ represent?

Theorem 3.28. *There exists an algebraic curve $Y(1)$, defined over $\mathbb{Q}$, which is a coarse moduli space for elliptic curves. For any algebraic space T, the set of maps $Hom(T, Y(1))$ corresponds to the set of isomorphism classes of families of elliptic curves over T.*

In particular, when we take $T = Y(1)$ itself, the identity map $\mathrm{id} : Y(1) \to Y(1)$ corresponds to a special family of elliptic curves, denoted $\mathcal{E}_{\mathrm{univ}} \to Y(1)$. This is called the **universal family of elliptic curves parameterized by** $Y(1)$.

Theorem 3.29.

1. *The algebraic curve $Y(1)$ can be defined by a polynomial equation with coefficients in $\mathbb{Q}$.*
2. *The set of complex points of this algebraic curve is biholomorphic to the Riemann surface $\Gamma(1)\backslash\mathbb{H}$.*
3. *Let $\pi : R\mathcal{E}_{univ} \to Y(1)$ be the universal family. The pushforward of the sheaf of relative holomorphic 1-forms, $\omega = R^1\pi_*\Omega^1$, is a line bundle on $Y(1)$ known as the Hodge bundle. Modular forms of weight k are global sections of its k-th tensor power, i.e., elements of $H^0(Y(1), \omega^{\otimes k})$.*

3.6 PM Problem Session

Problem 3.30. *Show that $\mathcal{O}(-1)$ is a non-trivial line bundle on $\mathbb{P}^1_{\mathbb{C}}$.*

Solution. A line bundle is trivial if and only if it admits a global, nowhere-vanishing holomorphic section. We will show that any global holomorphic sec-

tion of the tautological line bundle $\mathcal{O}(-1)$ over $\mathbb{P}^1_{\mathbb{C}}$ must have a zero, unless it is the zero section itself.

The total space of $\mathcal{O}(-1)$ is the subset $L = \{(\ell, P) \in \mathbb{P}^1_{\mathbb{C}} \times \mathbb{C}^2 \mid P \in \ell\}$. A global section s is a holomorphic map $s : \mathbb{P}^1_{\mathbb{C}} \to L$ of the form $s(\ell) = (\ell, v(\ell))$, where $v(\ell)$ is a vector in the line ℓ. To analyze such a section, we use the standard atlas for $\mathbb{P}^1_{\mathbb{C}}$, consisting of the open sets $U_0 = \{[1 : z] \mid z \in \mathbb{C}\}$ and $U_1 = \{[w : 1] \mid w \in \mathbb{C}\}$, with the transition map $w = 1/z$ on the overlap $U_0 \cap U_1$.

On the chart U_0, a line $\ell = [1 : z]$ is spanned by the vector $(1, z)$. A holomorphic section s can be locally represented by a holomorphic function $f : \mathbb{C} \to \mathbb{C}$, such that $s([1 : z]) = ([1 : z], f(z)(1, z))$. On the chart U_1, a line $\ell = [w : 1]$ is spanned by $(w, 1)$. The section is locally represented by a holomorphic function $g : \mathbb{C} \to \mathbb{C}$, such that $s([w : 1]) = ([w : 1], g(w)(w, 1))$.

For s to be a well-defined global section, the local representations must agree on the overlap $U_0 \cap U_1$. A point $[1 : z]$ in U_0 corresponds to $[1/z : 1]$ in U_1. The vector component $v(\ell)$ must be the same regardless of the chart. This yields the equality:

$$f(z)(1, z) = g(1/z)(1/z, 1).$$

Comparing the first components gives $f(z) = (1/z)g(1/z)$, which is equivalent to the transition relation $g(w) = wf(1/w)$ where $w = 1/z$.

For s to be a global holomorphic section, both local functions $f(z)$ and $g(w)$ must be entire. Let $f(z) = \sum_{n=0}^{\infty} a_n z^n$ be the power series expansion of f. The transition relation implies that the Laurent series for g around $w = 0$ is:

$$g(w) = w \sum_{n=0}^{\infty} a_n (1/w)^n = \sum_{n=0}^{\infty} a_n w^{1-n} = a_0 w + a_1 + a_2 w^{-1} + a_3 w^{-2} + \dots$$

For $g(w)$ to be entire, it must not have any terms with negative powers in its Laurent series. This forces $a_n = 0$ for all $n \geqslant 2$. Therefore, the function $f(z)$ must be a polynomial of degree at most 1, i.e., $f(z) = a_0 + a_1 z$ for some complex constants a_0, a_1. The corresponding function is then $g(w) = w(a_0 + a_1(1/w)) = a_0 w + a_1$. Both f and g are entire, as required.

Now we check for zeros of this global section. The section vanishes at a point if its local representative function is zero. If $a_1 \neq 0$, the section vanishes on U_0 where $f(z) = a_0 + a_1 z = 0$, i.e., at the point $[1 : -a_0/a_1]$. If $a_1 = 0$ but $a_0 \neq 0$, then $f(z) = a_0$ is nowhere zero on U_0. However, the corresponding local function on U_1 is $g(w) = a_0 w$, which vanishes at $w = 0$. The point $w = 0$ corresponds to the point $[0 : 1] \in \mathbb{P}^1_{\mathbb{C}}$. In every case where the section is not identically zero (i.e., where a_0 and a_1 are not both zero), it must have a zero somewhere on $\mathbb{P}^1_{\mathbb{C}}$. Since there are no non-vanishing global holomorphic sections, the line bundle $\mathcal{O}(-1)$ is non-trivial. □

Problem 3.31. *Show that* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the translation* $T(z) = z + 1$ *and the inversion* $S(z) = -1/z$. *Conclude that the* j*-invariant is a modular function for* $\mathrm{SL}_2(\mathbb{Z})$.

Solution. The statement that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is a standard and fundamental result in the theory of modular groups. The proof is typically achieved by showing that any matrix in $\mathrm{SL}_2(\mathbb{Z})$ can be reduced to the identity matrix by left-multiplying by powers of S and T, which is analogous to the Euclidean algorithm.

A modular function for $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ is a meromorphic function $f : \mathbb{H} \to \mathbb{C} \cup \{\infty\}$ that is invariant under the action of the group, i.e., $f(\gamma z) = f(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and is meromorphic at the cusp. To show the j-invariant is a modular function, it suffices to show it is invariant under the generators S and T.

Consider the action of the translation $T(z) = z + 1$. The corresponding lattice is $\Lambda_{\tau+1} = \mathbb{Z}(\tau + 1) \oplus \mathbb{Z}$. An arbitrary element of this lattice is $m(\tau + 1) + n = m\tau + (m + n)$ for $m, n \in \mathbb{Z}$. This is clearly an element of Λ_τ. Conversely, any element $m\tau + n \in \Lambda_\tau$ can be written as $m(\tau + 1) + (n - m)$, which is an element of $\Lambda_{\tau+1}$. Thus, the lattices are identical: $\Lambda_{\tau+1} = \Lambda_\tau$. Since the j-invariant depends only on the lattice structure, we have $j(\tau + 1) = j(\tau)$.

Next, consider the action of the inversion $S(z) = -1/z$. The corresponding lattice is $\Lambda_{-1/\tau} = \mathbb{Z}(-1/\tau) \oplus \mathbb{Z}$. This lattice is not identical to Λ_τ, but it is homothetic. We can scale $\Lambda_{-1/\tau}$ by the complex number $\tau \in \mathbb{C}^\times$:

$$\tau \cdot \Lambda_{-1/\tau} = \tau \cdot (\mathbb{Z}(-1/\tau) \oplus \mathbb{Z}) = \mathbb{Z}(-1) \oplus \mathbb{Z}\tau = \mathbb{Z}\tau \oplus \mathbb{Z} = \Lambda_\tau.$$

Two lattices Λ and Λ' are homothetic if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$. The j-invariant is a function on homothety classes, meaning $j(\Lambda') = j(\Lambda)$. In our case, this means $j(\Lambda_{-1/\tau}) = j(\tau \cdot \Lambda_{-1/\tau}) = j(\Lambda_\tau)$. Therefore, $j(-1/\tau) = j(\tau)$.

Since the j-invariant is invariant under the action of the generators S and T, it is invariant under the entire group $\mathrm{SL}_2(\mathbb{Z})$. The j-function is defined to be holomorphic on $\mathbb{H}$ and has a simple pole at the cusp $i\infty$, so it satisfies all the conditions of a modular function of level 1. □

Problem 3.32. *Give an example of two lattices which are not homothetic.*

Solution. Two lattices Λ_1 and Λ_2 are homothetic if and only if the elliptic curves they define, $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$, are isomorphic as Riemann surfaces. The isomorphism class of an elliptic curve is uniquely determined by its j-invariant. Therefore, to find two non-homothetic lattices, it suffices to find two lattices with different j-invariants. Each homothety class of lattices corresponds to a unique point in the modular curve $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$, which is parameterized by the j-invariant. We can thus select two points in the standard fundamental domain whose lattices will not be homothetic.

Consider the square lattice, $\Lambda_1 = \mathbb{Z}i \oplus \mathbb{Z}$. This lattice corresponds to the point $\tau = i \in \mathbb{H}$ and is associated with an elliptic curve with complex multiplication

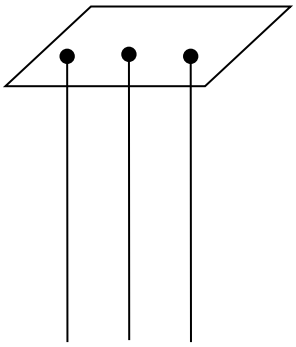
by $\mathbb{Z}[i]$. Its j-invariant is $j(i) = 1728$. Now, consider the hexagonal lattice, $\Lambda_2 = \mathbb{Z}e^{i\pi/3} \oplus \mathbb{Z}$. This corresponds to the point $\tau = e^{i\pi/3} \in \mathbb{H}$ and is associated with an elliptic curve with complex multiplication by the ring of Eisenstein integers $\mathbb{Z}[e^{i\pi/3}]$. For this lattice, the coefficient g_2 vanishes, which immediately implies its j-invariant is $j(e^{i\pi/3}) = 0$.

Since $j(\Lambda_1) = 1728$ and $j(\Lambda_2) = 0$, their j-invariants are unequal. Therefore, the square and hexagonal lattices are not homothetic. $\square$

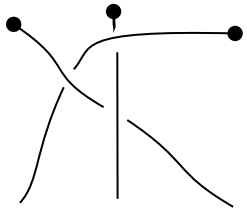
4 Thursday, June 5

4.1 AM Session 1: Braid Groups I

There are these **braided strands**:

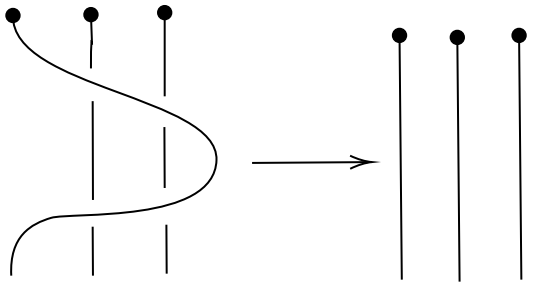


and we flip them around each other to form a **braid**:



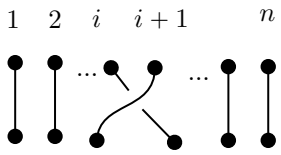
Definition 4.1. *Two braids are equivalent if there is a* ***isotopy*** *(smooth deformation) of one into the other, holding ends of strands constant.*

Example 4.2. *Here is an example of an isotopy. Given braids b_1, b_2, form their product $b_1 b_2$ by gluing the bottom of b_1 to the top of b_2:*



This forms a group. The trivial braid is an identity element for the product. Inverses are made by reflecting it over the bottom. After isotopy, we can make every crossing happen at a different height. This makes it clearly associative, so therefore n-stranded braids form a group B_n.

Therefore B_n is generated by elements of the form



for all $i = 1, ..., n-1$.

More formally:

Definition 4.3. *Pick points $p_1, ..., p_n \in \mathbb{C}$. A **braid** b is a collection of paths $\gamma_1 : [0,1] \to \mathbb{C} \times [0,1]$ for $i = 1, ..., n$, called **strands**, and a permutation $\overline{\gamma}$ of $\{1, ..., n\}$ such that*

1. *the strands $\gamma([0,1]) \subseteq \mathbb{C} \times [0,1]$ are disjoint*
2. *$\gamma_i(0) = (p_i, 0)$*
3. *$\gamma_i(1) = (p_{\overline{\gamma}(i)}, 1)$*
4. *$\gamma_i(t) = \mathbb{C} \times \{t\}$ for all $t \in [0,1]$.*

Then γ_i crosses γ_j at t if $\pi : \mathbb{C} \times [0,1] \to \mathbb{C}$ if there exists t such that $Re(\pi(\gamma_i(t))) = Re(\pi(\gamma_j(t)))$.

Definition 4.4. *A **braid diagram** is the projectioun of the images of γ_i onto $\mathbb{R} \times [0,1]$, with under/over crossing data.*

4.2 AM Session 2: Braid Groups II

Exercise 4.5. *Draw pictures of the relations*

$$\sigma_i \sigma_j = \sigma_j \sigma_i$$

if $|i-j| \geqslant 2$ and

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}.$$

Definition 4.6. *The **Artin braid group** is defined as*

$$A_n = \left\langle a_1, \ldots, a_{n-1} \;\middle|\; \begin{cases} a_i a_j a_i^{-1} a_j^{-1} & \text{if } |i-j| \geqslant 2, \\ a_i a_{i+1} a_i a_{i+1}^{-1} a_i^{-1} a_{i+1}^{-1} & \text{for } i = 1, \ldots, n-2 \end{cases} \right\rangle$$

This means that there is a surjective homomorphism

$$\begin{aligned} A_n &\xrightarrow{\varphi} B_n \\ a_i &\mapsto \sigma_i \end{aligned}$$

Proposition 4.7. *φ is an isomorphism.*

Define $\Psi : B_n \to A_n$ by: for a braid b, choose a isotopy into the form $b = (\sigma_{i_1})^{\epsilon_1} (\sigma_{i_2})^{\epsilon_2} ... (\sigma_{i_k})^{\epsilon_k}$ where $\epsilon_j = \pm 1$ for all j. Define $\Psi(b) = (a_{i_1})^{\epsilon_1} (a_{i_2})^{\epsilon_2} ... (a_{i_k})^{\epsilon_k}$.

Exercise 4.8. *Prove that Ψ is well-defined using the fact that any two isotopic braids have isomorphic braid diagrams that are related by isotopy of braid diagrams and Reidemeister moves.*

Corollary 4.9. *B_n has presentation*

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{cases} \sigma_i\sigma_j\sigma_i^{-1}\sigma_j^{-1} & \text{if } |i-j| \geqslant 2, \\ \sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1}^{-1} & \text{for } i = 1, \dots, n-2 \end{cases} \right\rangle$$

Example 4.10.

$$\begin{aligned} B_3 &\cong \langle \sigma_1, \sigma_2 | \sigma_1\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1} \rangle \\ &\cong \langle \sigma_1, \sigma_2 | \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1} \rangle \\ &= \langle x, \sigma_2 | x^3 \cdot x^{-1}\sigma_2^{-1}x^{-1}\sigma_2^{-1} \rangle \\ &= \langle x, y | x^3y^{-2} \rangle \end{aligned}$$

by substituting $x = \sigma_1\sigma_2$ and $y = \sigma_2 x$.

Exercise 4.11. *$\langle x, y | x^3y^{-2} \rangle \cong \mathbb{Z}_\mathbb{Z}\mathbb{Z}$ where $i_1 : \mathbb{Z} \hookrightarrow \mathbb{Z}, m \mapsto 3m$ and $i_2 : \mathbb{Z} \to \mathbb{Z}, m \mapsto 2m$. Therefore $Z(\langle x, y | x^3y^{-2} \rangle) = \langle x^3 \rangle = \langle y^2 \rangle$. Then*

$$\begin{aligned} B_3/Z(B_3) &\cong \langle x, y | x^3, y^2 \rangle \\ &\cong PSL_2(\mathbb{Z}) \end{aligned}$$

Exercise 4.12. *Check that*

$$\begin{aligned} B_n &\to S_n \\ b &\mapsto \overline{\gamma} \end{aligned}$$

is a homomorphism.

Definition 4.13. *The kernel is the **pure braid group** P_n, the subgroup where each strand begins and ends at the same place.*

Now we move onto discuss configuration spaces. Let $C^{\text{ord}}(\mathbb{C}, n) = \mathbb{C}\backslash\text{BigDiag}(\mathbb{C}^n)$ be the space of ordered n-tuples of distinct points in $\mathbb{C}$, where $\text{BigDiag}(\mathbb{C}^n) = \{(z_1, ..., z_n) \in \mathbb{C}^n | z_i = z_j \text{ for some } i \neq j\}$.

S_n acts on $C^{\text{ord}}(\mathbb{C}, n)$ by permuting coordinates. The space of orbits is the unordered configuration space $C(\mathbb{C}, n) = C^{\text{ord}}(\mathbb{C}, n)/S_n = \{S_n \cdot x | x \in C^{\text{ord}}(\mathbb{C}, n)\}$.

Observation: an element of B_n is a (isotopy class of) paths in $C(\mathbb{C}, n)$. The beginning and ending points are the same. Upshot: $B_k \cong \pi_1(C(\mathbb{C}, n))$.

4.3 AM Problem Session

Problem 4.14. *Suppose a group G acts on a set X, and let $Z(G)$ be the center of G. Show that if $z \in Z(G)$ and $g \in G$ then the action of z preserves the set of*

fixed points of g fixed by the action of g. Use this along with the amalgamated product description of the braid group B_n to prove that the center of B_n is the cyclic subgroup generated by $(\sigma_1\sigma_2\dots\sigma_n)^n$.

Solution. Let $g \in G$ and let $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ be its set of fixed points. Let $z \in Z(G)$, meaning $zg = gz$ for all $g \in G$. We must show that the action of z maps the set $\mathrm{Fix}(g)$ to itself. Let $x \in \mathrm{Fix}(g)$. We check if the point $z \cdot x$ is also fixed by g.

$$g \cdot (z \cdot x) = (gz) \cdot x = (zg) \cdot x = z \cdot (g \cdot x).$$

Since $x \in \mathrm{Fix}(g)$, we have $g \cdot x = x$. Substituting this gives:

$$z \cdot (g \cdot x) = z \cdot x.$$

Thus, $g \cdot (z \cdot x) = z \cdot x$, which shows that $z \cdot x$ is also a fixed point of g. Therefore, the action of any central element z preserves the fixed-point set of any other group element. □

Problem 4.15. *If a group is given by a presentation $G \cong \langle S \mid R\rangle$ then the abelianization of G is the quotient group with presentation $\langle S \mid R \cup A\rangle$, where A is the subset of G consisting of all commutators of elements of S. (The commutator of $x, y \in S$ is the group element $xyx^{-1}y^{-1}$.) Show that the abelianization of B_n is isomorphic to $\mathbb{Z}$ and describe the homomorphism.*

Solution. The braid group B_n has the presentation $\langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2; \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}\rangle$. To find the abelianization $B_n^{ab} = B_n/[B_n, B_n]$, we add relations forcing all generators to commute, i.e., $\sigma_i\sigma_j = \sigma_j\sigma_i$ for all i, j.

The first set of relations, $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geqslant 2$, is now subsumed by the general commutativity relations. The crucial braid relation becomes:

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}.$$

Since all generators commute in the abelianization, we can reorder the terms:

$$\sigma_i^2\sigma_{i+1} = \sigma_i\sigma_{i+1}^2.$$

Since we are in a group, we can cancel one σ_i and one σ_{i+1} from each side, which yields:

$$\sigma_i = \sigma_{i+1}.$$

This holds for all $i = 1, \dots, n-2$. By transitivity, this implies that in the abelianization, the images of all generators are equal: $\sigma_1 = \sigma_2 = \cdots = \sigma_{n-1}$. Let σ be the common image of all σ_i in B_n^{ab}. The group B_n^{ab} is generated by the single element σ. There are no remaining relations that constrain σ (e.g., of the form $\sigma^k = e$). Therefore, the abelianization is the free group on one generator, which is the infinite cyclic group $\mathbb{Z}$.

The homomorphism $B_n \to \mathbb{Z}$ is the map that sends each generator σ_i to the generator $1 \in \mathbb{Z}$. For an arbitrary braid word $w = \sigma_{i_1}^{\epsilon_1} \dots \sigma_{i_k}^{\epsilon_k}$, the homomorphism is the exponent sum map, which counts the total number of positive crossings minus the total number of negative crossings, regardless of which strands are involved: $\varphi(w) = \sum_{j=1}^{k} \epsilon_j$. □

Problem 4.16. *Show that the generators σ_i of the braid group B_n are all conjugate to each other. Then show that the conjugate of $\gamma = \sigma_i\sigma_j$ by $\delta = \sigma_k\sigma_l\sigma_p$ is equal to γ^{-1}. (That is, show that $\delta\gamma\delta^{-1} = \gamma^{-1}$.)*

Solution. We will show that σ_i is conjugate to σ_{i+1} for any $i = 1, \dots, n-2$. By transitivity, this implies all generators σ_i lie in the same conjugacy class. We use the braid relation $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$. We can isolate σ_{i+1} from this relation. Starting with the right-hand side, we multiply by σ_{i+1}^{-1} on the right:

$$(\sigma_i\sigma_{i+1}\sigma_i)\sigma_{i+1}^{-1} = \sigma_{i+1}\sigma_i.$$

Now, multiply by σ_i^{-1} on the right:

$$(\sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1}^{-1})\sigma_i^{-1} = \sigma_{i+1}.$$

This gives the expression $\sigma_{i+1} = (\sigma_i\sigma_{i+1})\sigma_i(\sigma_i\sigma_{i+1})^{-1}$. This is precisely the statement that σ_{i+1} is the conjugate of σ_i by the element $\sigma_i\sigma_{i+1}$. Since this holds for all adjacent indices i and $i+1$, all generators $\sigma_1, \dots, \sigma_{n-1}$ are mutually conjugate. □

Problem 4.17. *Show that S_n has presentation $\langle \tau_1, \tau_2, \dots, \tau_{n-1} \mid R \rangle$, where R consists of relations $\tau_i\tau_j = \tau_j\tau_i$ for all $|i-j| > 1$, relations $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ for $i = 1, \dots, n-2$, and involution relations τ_i^2 for all i.*

Solution. This is the standard Coxeter presentation for the symmetric group. Let G be the group defined by this presentation. Let τ_i correspond to the adjacent transposition $(i, i+1)$ in S_n.

First, we verify that the generators of S_n satisfy the relations. The transpositions are involutions, so $(i, i+1)^2 = e$, satisfying $\tau_i^2 = e$. If $|i-j| > 1$, the transpositions $(i, i+1)$ and $(j, j+1)$ act on disjoint sets of elements, so they commute, satisfying $\tau_i\tau_j = \tau_j\tau_i$. Finally, one can directly compute the braid relation: $(i, i+1)(i+1, i+2)(i, i+1) = (i, i+2) = (i+1, i+2)(i, i+1)(i+1, i+2)$. Thus, the generators of S_n satisfy all the relations of G. By the universal property of group presentations (von Dyck's theorem), this implies there is a surjective homomorphism $\phi : G \to S_n$.

To prove that ϕ is an isomorphism, we must show it is injective, which is equivalent to showing that $|G| \leqslant |S_n| = n!$. This is typically done by an induction argument or a coset enumeration (Schreier-Todd-Coxeter algorithm). Let G_{n-1} be the subgroup of G generated by $\{\tau_1, \dots, \tau_{n-2}\}$. By the presentation, this is a

group of the same type for $n-1$. Assuming inductively that $|G_{n-1}| \leqslant (n-1)!$, one considers the cosets of G_{n-1} in G_n. Using the relations, one can show that any element of G_n can be written in the form $g\tau_{n-1}\tau_{n-2}\dots\tau_k$ for some k, where $g \in G_{n-1}$. This analysis shows there are at most n distinct left cosets, so $|G_n| \leqslant n|G_{n-1}|$. By induction, this gives $|G_n| \leqslant n!$. Since we have a surjective homomorphism from G to S_n and the order of G is at most the order of S_n, the homomorphism must be an isomorphism. □

Problem 4.18.

1. *Check that the assignment $\sigma_i \mapsto \sigma_i$ for each $i = 1, \dots, n-1$ defines an injective homomorphism $i : B_n \to B_{n+1}$. (Use the geometric description of the braid group.)*
2. *Can you define a reasonable function $B_n \to B_n$? Is it a homomorphism?*
3. *The map $i : B_n \to B_{n+1}$ restricts to an injective homomorphism $j : P_n \to P_{n+1}$. Show that 'forget the last strand' defines a homomorphism $q : P_{n+1} \to P_n$ satisfying $q \circ i = id_{P_n}$. Conclude that P_{n+1} is the semidirect product of P_n and U_{n+1}, the kernel of q. (In fact, U_{n+1} is isomorphic to a free group. This can be used to show that P_n has no finite-order elements.)*

Solution.

1. The map $i : B_n \to B_{n+1}$ defined on the generators by $i(\sigma_j) = \sigma_j$ for $j = 1, \dots, n-1$ is an injective homomorphism. Geometrically, this map takes an n-strand braid and adds a new, $(n+1)$-th strand to the right that runs straight down without interacting with the others. Since the relations for B_n only involve generators with indices up to $n-1$, these relations are preserved under the mapping into B_{n+1}. The map is injective because if a non-trivial n-strand braid were to become trivial after adding a straight strand, it would imply the original braid was trivial, as the added strand does not create any new possibility for undoing the existing crossings.
2. Consider the map $\rho : B_n \to B_n$ defined by the geometric action of rotating a braid by 180° around a central vertical axis. This transformation sends the k-th strand to the $(n-k+1)$-th position. Consequently, the generator σ_i, representing a crossing of strands i and $i+1$, is mapped to a crossing of strands $n-i$ and $n-i+1$. On the generators, the map is defined as:

$$\rho(\sigma_i) = \sigma_{n-i} \quad \text{for } i = 1, \dots, n-1$$

   Now, we verify that it preserves the defining relations of B_n.

   (a) Commutation Relation: For $|i-j| \geqslant 2$, we must check if $\rho(\sigma_i\sigma_j) = \rho(\sigma_j\sigma_i)$. Applying ρ gives $\sigma_{n-i}\sigma_{n-j} = \sigma_{n-j}\sigma_{n-i}$. This relation holds because the absolute difference of the new indices, $|(n-i)-(n-j)| = |i-j|$, remains $\geqslant 2$.

(b) Braid Relation: For $1 \leqslant i \leqslant n-2$, we check if $\rho(\sigma_i\sigma_{i+1}\sigma_i) = \rho(\sigma_{i+1}\sigma_i\sigma_{i+1})$. Applying ρ yields:

$$\sigma_{n-i}\sigma_{n-(i+1)}\sigma_{n-i} = \sigma_{n-(i+1)}\sigma_{n-i}\sigma_{n-(i+1)}$$

Let $k = n-i-1$, which implies $n-i = k+1$. The equation becomes $\sigma_{k+1}\sigma_k\sigma_{k+1} = \sigma_k\sigma_{k+1}\sigma_k$. This is the standard braid relation for index k. Since $1 \leqslant i \leqslant n-2$, the new index k falls within the valid range $[1, n-2]$, so the relation is preserved.

Since ρ preserves the defining relations, it is a homomorphism. Furthermore, as $\rho(\rho(\sigma_i)) = \rho(\sigma_{n-i}) = \sigma_{n-(n-i)} = \sigma_i$, the map is its own inverse, making it an automorphism of B_n.

3. The map $q : P_{n+1} \to P_n$, defined geometrically by "forgetting the last strand," is a homomorphism for pure braid groups. The kernel of this map, $\ker(q)$, consists of pure braids on $n+1$ strands where the first n strands are straight and the $(n+1)$-th strand weaves among them before returning to its starting position. The composition $q \circ i$ where $i : P_n \to P_{n+1}$ is the inclusion from part (a) is clearly the identity on P_n. A surjective homomorphism q that has a right inverse i is called a retraction. The existence of a retraction implies that the group P_{n+1} is a semidirect product of the kernel of q and the image of i. Thus, $P_{n+1} \cong \ker(q) \rtimes \mathrm{Im}(i) \cong \ker(q) \rtimes P_n$. The kernel, which describes the motion of a single point (the $(n+1)$-th strand) in the plane punctured by n fixed points (the other strands), is isomorphic to the fundamental group of a punctured plane, which is the free group on n generators, F_n.

□

Problem 4.19. *Show that the full twist*

$$\theta_n = ((\sigma_1\sigma_2\ldots\sigma_{n-1})(\sigma_1\sigma_2\ldots\sigma_{n-2})\ldots(\sigma_1\sigma_2)\sigma_1)^2$$

is in the center of the braid group B_n. (In fact, this element generates the center of both B_n and P_n, but it's a bit harder to show.)

Solution. The element described, which should be the square of the Garside half-twist Δ_n, is the full twist braid $\theta_n = \Delta_n^2$. The Garside element is $\Delta_n = (\sigma_1\sigma_2\ldots\sigma_{n-1})(\sigma_1\sigma_2\ldots\sigma_{n-2})\ldots(\sigma_1)$. To show that $\theta_n = \Delta_n^2$ is in the center of B_n, we must show it commutes with all generators σ_j for $j = 1, \ldots, n-1$. A key property of the Garside element is the conjugation relation $\sigma_i\Delta_n = \Delta_n\sigma_{n-i}$. We compute the conjugate of Δ_n by itself:

$$\Delta_n\Delta_n\Delta_n^{-1} = \Delta_n.$$

Conjugating the relation $\sigma_i\Delta_n = \Delta_n\sigma_{n-i}$ by Δ_n gives:

$$\Delta_n(\sigma_i\Delta_n)\Delta_n^{-1} = \Delta_n(\Delta_n\sigma_{n-i})\Delta_n^{-1} \implies (\Delta_n\sigma_i) = (\sigma_{n-(n-i)})(\Delta_n) = \sigma_i\Delta_n.$$

Wait, this is not the proof. The standard proof is geometric. The element Δ_n^2 corresponds to a braid where each strand makes a full twist around all the other strands. Geometrically, this operation is symmetric with respect to all strands and can be continuously deformed to the boundary of the braid diagram. Conjugating σ_j by Δ_n^2 means performing a full twist, then the crossing σ_j, then undoing the full twist. The result is isotopically equivalent to simply performing the crossing σ_j. Thus, $\Delta_n^2 \sigma_j \Delta_n^{-2} = \sigma_j$, which implies $\Delta_n^2 \sigma_j = \sigma_j \Delta_n^2$. As it commutes with all generators, it is in the center of B_n. □

Problem 4.20. *Complete the following outline to prove that if B_n is isomorphic to B_m, then $n = m$. First check that an isomorphism of groups induces isomorphisms of their centers and of their abelianizations. Then check that Image of $Z(B_n)$ in the abelianization of B_n is a subgroup of index $n(n-1)$.*

Solution. This result is known as the Artin-Tits conjecture, proven by solving the isomorphism problem for braid groups. The argument outlined provides a beautiful proof of this fact. Let $\phi : B_n \to B_m$ be an isomorphism. Any group isomorphism induces an isomorphism between the centers of the groups, $\phi_Z : Z(B_n) \to Z(B_m)$, and also an isomorphism between their abelianizations, $\phi_{ab} : B_n^{ab} \to B_m^{ab}$.

From previous problems, we know that the abelianization B_k^{ab} is isomorphic to $\mathbb{Z}$, via the exponent-sum map $\pi_k : B_k \to \mathbb{Z}$ which sends each generator σ_i to 1. We also know that the center $Z(B_k)$ is an infinite cyclic group generated by the full twist braid $\theta_k = \Delta_k^2$.

Let us compute the image of the generator of the center under the abelianization map. The Garside element Δ_k is the product $(\sigma_1 \dots \sigma_{k-1})(\sigma_1 \dots \sigma_{k-2}) \dots (\sigma_1)$. Its image in the abelianization is the sum of the exponents of its generators. The number of generators in Δ_k is the $(k-1)$-th triangular number, $\sum_{j=1}^{k-1} j = \frac{k(k-1)}{2}$. The generator of the center is $\theta_k = \Delta_k^2$. Its image under the abelianization map π_k is therefore $2 \cdot \frac{k(k-1)}{2} = k(k-1)$. The image of the center, $\pi_k(Z(B_k))$, is the subgroup of $B_k^{ab} \cong \mathbb{Z}$ generated by the element $k(k-1)$. This is the subgroup $k(k-1)\mathbb{Z}$.

The index of this subgroup in $\mathbb{Z}$ is $|\mathbb{Z}/k(k-1)\mathbb{Z}| = k(k-1)$. Since the isomorphism ϕ induces isomorphisms on the centers and abelianizations, it must preserve the index of the image of the center in the abelianization. Therefore, we must have:

$$n(n-1) = m(m-1).$$

The function $f(x) = x(x-1)$ is strictly increasing for $x \geqslant 1$. Thus, for integers $n, m \geqslant 2$, the equality $n(n-1) = m(m-1)$ implies that $n = m$. This proves that braid groups on different numbers of strands are not isomorphic. □

Problem 4.21. *What is the configuration space of two points on a circle? Three points on a closed interval?*

Solution. The ordered configuration space of k points in a topological space X, denoted $C^{\mathrm{ord}}(X,k)$, is the set of ordered k-tuples of distinct points in X.

For two points on a circle S^1, the space is $C^{\mathrm{ord}}(S^1,2) = \{(z_1,z_2) \in S^1 \times S^1 \mid z_1 \neq z_2\}$. This space is the product of the first point's position, S^1, and the possible positions of the second point, which is S^1 minus one point. The space $S^1 \backslash \{\mathrm{pt}\}$ is homeomorphic to an open interval. Therefore, $C^{\mathrm{ord}}(S^1,2)$ is homeomorphic to $S^1 \times (0,1)$, which is an open cylinder or annulus.

For three points on a closed interval $[0,1]$, the space is $C^{\mathrm{ord}}([0,1],3) = \{(x_1,x_2,x_3) \in [0,1]^3 \mid x_i \neq x_j \text{ for } i \neq j\}$. This is the unit cube with the three diagonal planes $x_1 = x_2$, $x_1 = x_3$, and $x_2 = x_3$ removed. The space of unordered configurations is often of more interest. For three points in $[0,1]$, we can enforce an order, say $0 \leqslant x_1 < x_2 < x_3 \leqslant 1$. This space is a subset of $\mathbb{R}^3$ defined by these inequalities. This region is the interior of a standard 3-simplex (a tetrahedron) with vertices at $(0,0,0),(1,1,1),(0,0,1),(0,1,1)$. Specifically, it is the open region defined by the vertices $(0,0,0)$, $(1,1,1)$, and permutations, which forms a tetrahedron. □

4.4 PM Session 1: Complex Multiplication I

A central goal of algebraic number theory is to understand the structure of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A key strategy is to study its abelian quotients by constructing and classifying the abelian extensions of $\mathbb{Q}$. This is the primary aim of class field theory.

A finite field extension $K/\mathbb{Q}$ is a number field. The extension is Galois if $|\operatorname{Aut}_{\mathbb{Q}}(K)| = [K:\mathbb{Q}]$. It is an abelian extension if the Galois group $\operatorname{Aut}_{\mathbb{Q}}(K)$ is abelian.

Exercise 4.22. *Let ζ_n be a primitive n-th root of unity.*

1. *Show that the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$.*
2. *Prove that its Galois group is isomorphic to the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$:*
$$\operatorname{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

The study of cyclotomic fields provides a complete description of the abelian extensions of $\mathbb{Q}$.

Theorem 4.23 (Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_n)$ for some integer $n \geqslant 1$.*

The Kronecker-Weber theorem can be rephrased through a more structural lens. The primitive roots of unity are the torsion points of the multiplicative group $\mathbb{C}^{\times}$. The theorem states that the maximal abelian extension of $\mathbb{Q}$, denoted $\mathbb{Q}^{ab}$, is generated by adjoining all such torsion points: $\mathbb{Q}^{ab} = \mathbb{Q}(\mu_\infty)$, where μ_∞ is the group of all roots of unity. This construction is related to the endomorphism ring of the algebraic group $\mathbb{G}_m \cong \mathbb{C}^{\times}$. Its endomorphism ring is $\mathrm{End}(\mathbb{G}_m) \cong \mathbb{Z}$, where the integer n corresponds to the endomorphism $z \mapsto z^n$.

Hilbert's twelfth problem asks for an explicit description of the abelian extensions of an arbitrary number field K. The theory of complex multiplication provides the answer for imaginary quadratic fields, using elliptic curves in place of the multiplicative group $\mathbb{G}_m$. To generate field extensions, one considers the coordinates of torsion points on an elliptic curve E, which form the torsion subgroup $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$. The structure of the endomorphism ring $\mathrm{End}(E)$ is fundamental to this theory.

An endomorphism of an elliptic curve $E = \mathbb{C}/\Lambda$ is a holomorphic group homomorphism $\phi : E \to E$. Such a map lifts to a holomorphic map $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$ of the form $\tilde{\phi}(z) = \alpha z$ for some $\alpha \in \mathbb{C}$. For $\tilde{\phi}$ to descend to the quotient, it must preserve the lattice. This gives a concrete description of the endomorphism ring:

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}.$$

This set is a subring of $\mathbb{C}$. It always contains $\mathbb{Z}$, since $n\Lambda \subseteq \Lambda$ for any $n \in \mathbb{Z}$. An elliptic curve is said to have complex multiplication if this containment is proper, i.e., if $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

Example 4.24. *Let $E = \mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}i \oplus \mathbb{Z}$. Then $i\Lambda = i(\mathbb{Z}i \oplus \mathbb{Z}) = \mathbb{Z}(-1) \oplus \mathbb{Z}i = \Lambda$, so the inclusion $i\Lambda \subseteq \Lambda$ holds. It follows that the ring of Gaussian integers $\mathbb{Z}[i]$ is a subring of End(E). Since $\mathbb{Z}$ is a proper subring of $\mathbb{Z}[i]$, the endomorphism ring of E is strictly larger than $\mathbb{Z}$. Therefore, E is an elliptic curve with complex multiplication.*

The rings that appear as endomorphism rings of CM elliptic curves are orders in imaginary quadratic fields. Let $K = \mathbb{Q}(\sqrt{-D})$ for a square-free integer $D > 0$.

Definition 4.25. *An **order** in an imaginary quadratic field K is a subring $\mathcal{O} \subset K$ that is also a free $\mathbb{Z}$-module of rank 2.*

For example, $\mathcal{O} = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ for some basis $\{w_1, w_2\}$.

Example 4.26. *The ring of Gaussian integers $\mathbb{Z}[i]$ is an order in the field $\mathbb{Q}(i)$.*

Lemma 4.27. *The set of all algebraic integers in K, denoted $\mathcal{O}_K$, forms an order called the **maximal order** of K. Every other order $\mathcal{O}$ in K is a subring of $\mathcal{O}_K$ of the form $\mathbb{Z} \oplus \mathbb{Z}f\omega$, where $f \geqslant 1$ is an integer called the conductor and $\{1, \omega\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$.*

4.5 PM Session 2: Complex Multiplication II

Proposition 4.28. *Let $E = \mathbb{C}/\Lambda$ be an elliptic curve. Its endomorphism ring End(E) is isomorphic to either $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field.*

Sketch of Proof. Let the lattice be $\Lambda = \mathbb{Z}\tau \oplus \mathbb{Z}$ for some $\tau \in \mathbb{H}$. An endomorphism $\alpha \in \mathrm{End}(E)$ must map Λ into itself. Thus, $\alpha \cdot 1 = a\tau + b$ and $\alpha \cdot \tau = c\tau + d$ for some integers a, b, c, d. From the first equation, $\alpha = a\tau + b$. Substituting this into the second gives $(a\tau+b)\tau = c\tau+d$, which rearranges to $a\tau^2+(b-d)\tau-c = 0$.

If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, there exists an endomorphism $\alpha \notin \mathbb{Z}$, for which we must have $a \neq 0$. This implies that τ is a root of a quadratic polynomial with integer coefficients. Since $\tau \in \mathbb{H}$, $\mathbb{Q}(\tau)$ must be an imaginary quadratic field. The ring $\mathrm{End}(E)$ is then an order in this field. It can be shown that any endomorphism α is an algebraic integer satisfying the characteristic polynomial $x^2 - (a+d)x + (ad - bc) = 0$. □

The theory of complex multiplication classifies elliptic curves with a specified endomorphism ring $\mathcal{O}$. For a maximal order $\mathcal{O}_K$ in an imaginary quadratic field K, the curve $E = \mathbb{C}/\mathcal{O}_K$ has $\mathrm{End}(E) = \mathcal{O}_K$.

The number of non-isomorphic elliptic curves with CM by a given order $\mathcal{O}_K$ is determined by the class group of that order.

Definition 4.29. *The **ideal class group** of a Dedekind domain $\mathcal{O}_K$, denoted $Cl(\mathcal{O}_K)$, is the quotient group of fractional ideals by principal fractional ideals. Its order, the class number h_K, measures the failure of unique factorization of elements.*

Example 4.30. *For the rational integers $\mathbb{Z}$, every ideal is principal. Thus, $Cl(\mathbb{Z})$ is the trivial group, $\{e\}$.*

Theorem 4.31. *The ideal class group $Cl(\mathcal{O}_K)$ is a finite abelian group.*

The main theorem of complex multiplication connects the arithmetic of $\mathcal{O}_K$ to the geometry of elliptic curves.

Theorem 4.32. *There is a bijection between the set of isomorphism classes of elliptic curves with $End(E) \cong \mathcal{O}_K$ and the elements of the ideal class group $Cl(\mathcal{O}_K)$. The correspondence maps an ideal class $[I]$ to the isomorphism class of the elliptic curve $\mathbb{C}/I$.*

Corollary 4.33. *For any maximal order $\mathcal{O}_K$ in an imaginary quadratic field, there are finitely many isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_K$. This number is the class number $h_K = |Cl(\mathcal{O}_K)|$.*

The connection between the class group of an imaginary quadratic order and the isomorphism classes of elliptic curves with complex multiplication by that order is the gateway to some of the most important results in number theory. These theorems form the foundation of the explicit class field theory for imaginary quadratic fields. The finiteness of the class number, a purely arithmetic fact, implies that there are only a finite number of distinct j-invariants corresponding to elliptic curves with a given CM type. This finiteness has many arithmetic consequences for the nature of these j-invariants themselves, which we explore in the following corollary.

Corollary 4.34. *Let E be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Then its j-invariant, $j(E)$, is an algebraic integer.*

Sketch of Proof. Let $j(E)$ be the j-invariant of a CM elliptic curve E, and let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Applying σ to the coefficients of a Weierstrass equation for E defines a new elliptic curve E^σ. The endomorphism rings are isomorphic, $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma)$, so E^σ also has CM by the same order. By the main theorem, there are only finitely many isomorphism classes of such curves. Therefore, the set $\{E^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{C})\}$ is finite. The j-invariant transforms as $j(E^\sigma) = \sigma(j(E))$. This means the set of all Galois conjugates of $j(E)$ is a finite set, which implies that $j(E)$ is an algebraic number. It is, in fact, an algebraic integer. Furthermore, the field extension $K(j(E))$ is the Hilbert class field of K - its maximal unramified abelian extension, with Galois group $\mathrm{Gal}(K(j(E))/K) \cong \mathrm{Cl}(\mathcal{O}_K)$. □

4.6 PM Problem Session

There were no problems.

5 Friday, June 6

5.1 AM Session 1: Mapping Class Groups

Recall that a braid is an isotopy class of paths in the configuration space $C(\mathbb{C}, n) = C(\mathbb{D}, n)$. Now, imagine that the disk $\mathbb{D}$ is made of a malleable material, like putty. Let $p_1, p_2, p_3, p_4 \in \mathbb{D}$ be four marked points. As these points move within the disk, they drag the surrounding putty with them. By the end of this motion (thought of as a continuous deformation over time) the resulting transformation of the disk determines a homeomorphism

$$f : \overline{\mathbb{D}} \to \overline{\mathbb{D}}$$

satisfying the following conditions:

1. $f(\{p_1, \ldots, p_n\}) = \{p_1, \ldots, p_n\}$ (preserves the set of marked points),
2. $f|_{\partial\overline{\mathbb{D}}} = \mathrm{id}_{\partial\overline{\mathbb{D}}}$ (fixes the boundary pointwise).

The collection of such transformations, up to isotopy, forms a group known as the mapping class group.

Definition 5.1. *The **mapping class group** of the n-punctured disk, denoted $Mod(\overline{\mathbb{D}}, n)$, is the group of isotopy classes of homeomorphisms $f : \overline{\mathbb{D}} \to \overline{\mathbb{D}}$ such that f preserves the set of marked points, $\{p_1, \ldots, p_n\}$, and fixes the boundary $\partial\overline{\mathbb{D}}$ pointwise.*

Theorem 5.2. *There is a canonical isomorphism between the braid group on n strands and the mapping class group of the n-punctured disk:*

$$B_n \cong Mod(\overline{\mathbb{D}}, n).$$

We can similarly define the mapping class group of any compact, orientable surface S.

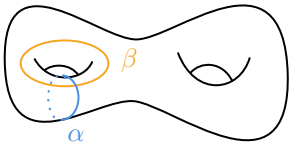
The elements of mapping class groups can be understood through fundamental building blocks. A primary class of such elements are Dehn twists, which are associated with simple closed curves on the surface.

Definition 5.3. *A **simple closed curve** on a surface S is an embedding of S^1 into S. A **homotopy** between curves is a continuous deformation that allows self-intersection.*

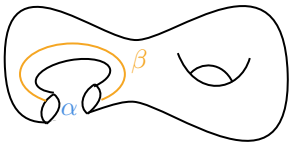
A Dehn twist about a simple closed curve α is constructed by cutting the surface along α, twisting one of the resulting boundaries by a full 360°, and re-gluing. The resulting homeomorphism is denoted T_α.

Now we describe the Dehn twist:

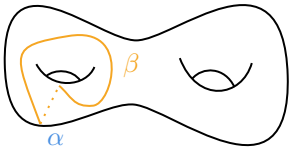
1. Choose homotopically nontrivial simple closed curve.



2. Cut along α.



3. Choose a cuff, twist it 2π to the right, and then reglue.



The interaction between Dehn twists is governed by the topology of the underlying curves. This gives rise to the algebraic relations in the mapping class group.

Exercise 5.4. *Let α and β be two simple closed curves. Show that $T_{T_\beta(\alpha)} = T_\beta T_\alpha T_\beta^{-1}$. Use this to show that if $T_\beta(\alpha)$ is isotopic to $T_\alpha^{-1}(\beta)$, then the braid relation $T_\alpha T_\beta T_\alpha = T_\beta T_\alpha T_\beta$ holds.*

Corollary 5.5. *The braid relation is*

$$T_\alpha T_\beta T_\alpha = T_\beta T_\alpha T_\beta$$

Proof. We begin by noting the following two facts:

1. For any $f \in \mathrm{Mod}(S)$ and any simple closed curve a on S, we have

$$T_{f(a)} = f \circ T_a \circ f^{-1}.$$

2. For any simple closed curves c and d, we have

$$T_c = T_d \quad \text{if and only if} \quad c \simeq d,$$

where $\simeq$ denotes homotopy.

Now, observe that

$$\begin{aligned} T_\beta &= T_{(T_\alpha T_\beta)(\alpha)} \\ &= (T_\alpha T_\beta) \circ T_\alpha \circ (T_\alpha T_\beta)^{-1}, \end{aligned}$$

where the first equality uses fact (2) and the second follows from fact (1). □

Definition 5.6. *Let $i(\alpha, \beta)$ be the **geometric intersection number**, defined as the minimal number of transverse intersections among all curves isotopic to α and β.*

Proposition 5.7. *Assume α and β represent distinct isotopy classes. The structure of the subgroup $\langle T_\alpha, T_\beta \rangle$ generated by two Dehn twists depends on their intersection number:*

- *If $i(\alpha, \beta) = 0$, the curves are disjoint, and the Dehn twists commute: $\langle T_\alpha, T_\beta \rangle \cong \mathbb{Z} \times \mathbb{Z}$.*
- *If $i(\alpha, \beta) = 1$, the twists satisfy the braid relation: $\langle T_\alpha, T_\beta \rangle \cong B_3$.*
- *If $i(\alpha, \beta) \geqslant 2$, the twists typically generate a free group, $\langle T_\alpha, T_\beta \rangle \cong F_2$.*

5.2 AM Session 2: Rational Tangles I

The theory of rational tangles helps tie in all of the stories we've seen together. A rational tangle is an isotopy class of a 2-tangle, which can be visualized as two ropes with four endpoints fixed at the corners of a square. Two fundamental operations, a horizontal Twist (T) and a vertical Rotation (R), can be applied. A theorem of Conway and Kauffman states that any rational tangle can be undone by a sequence of these moves.

This is proven by assigning a rational number (or ∞) to each tangle, its tangle invariant τ. The untangled state has $\tau = 0$. The operations correspond to transformations on this number:

- $\tau(T \cdot \sigma) = \tau(\sigma) + 1$
- $\tau(R \cdot \sigma) = -1/\tau(\sigma)$

These correspond to Möbius transformations of the extended rational line $\mathbb{Q} \cup \{\infty\}$, induced by the generators

$$T \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

which generate the group $\mathrm{PSL}_2(\mathbb{Z})$. Thus, the invariant τ realizes an isomorphism between the group action on tangles and that of Möbius transformations on the projective line. The process of untangling then corresponds to applying the Euclidean algorithm to the rational number $\tau(\sigma)$.

Example 5.8. *The following sequence of operations untangles a tangle with invariant* $\frac{27}{19}$*:*

$$\frac{27}{19} \xrightarrow{R} \frac{-19}{27} \xrightarrow{T} \frac{8}{27} \xrightarrow{R} \frac{-27}{8} \xrightarrow{T^4} \frac{5}{8} \xrightarrow{R} \frac{-8}{5} \xrightarrow{T^2} \frac{2}{5} \xrightarrow{R} \frac{-5}{2} \xrightarrow{T^3} \frac{1}{2} \xrightarrow{R} -2 \xrightarrow{T^2} 0$$

Proposition 5.9. *If* $\tau(\sigma) = 0$*, then* σ *is isotopic to the untangle.*

Proof. Let $\mathcal{T}$ denote the set of rational tangles and $\Gamma = F_2 = \langle R, T \rangle$ the free group on the two operations. There are two natural group actions:

1. $\Gamma \curvearrowright \mathcal{T}$ via composition of tangle operations;
2. $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{Q} \cup \{\infty\}$ via Möbius transformations, where:

$$z \xmapsto{T} z+1 \quad \text{corresponds to} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad z \xmapsto{R} -\frac{1}{z} \quad \text{corresponds to} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Let $\phi : F_2 \to \mathrm{PSL}_2(\mathbb{Z})$ denote the natural homomorphism. If $\sigma = W \cdot \sigma_0$ and $\tau(\sigma) = 0$, then $\phi(W) \cdot 0 = 0$, so $\phi(W) \in \mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(0)$. Thus, $W \in \phi^{-1}(\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(0)) = \mathrm{Stab}^{(2)}_{F_2}(0)$. □

Let's talk about symmetries.

Definition 5.10. *The* ***bdpq symmetry*** *of a tangle refers to a geometric* $\mathbb{Z}/2 \times \mathbb{Z}/2$ *symmetry under rotation and reflection. Label the four endpoints of the tangle diagram as b (bottom left), d (bottom right), p (top right), and q (top left). A quarter-turn rotation cyclically permutes these labels according to the transformation rules:* $b \to d$*,* $d \to p$*,* $p \to q$*,* $q \to b$*.*

Proposition 5.11. *Every rational tangle admits a bdpq symmetry.*

Proof. Proceed by induction on the number of operations used to generate a tangle from the untangle.

Base case: The untangle clearly exhibits bdpq symmetry.

Inductive step: Suppose σ has bdpq symmetry. Then $T \circ \sigma$ and $R \circ \sigma$ also preserve this symmetry, since the operations T and R act equivariantly with respect to the diagram's geometric symmetry group. □

Suppose $\sigma \in \mathcal{T}$ satisfies $\tau(\sigma) = 0$. Then $\sigma = W \cdot \sigma_0$, for some $W \in F_2$, and $\phi(W) \cdot 0 = 0$, so $W \in \mathrm{Stab}^{(2)}_{F_2}(0) := \phi^{-1}(\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(0))$. There are two types of elements in this preimage:

1. Preimages of generators in $\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(0)$;
2. Elements in $\ker\phi$, the kernel of the homomorphism $F_2 \to \mathrm{PSL}_2(\mathbb{Z})$.

To analyze the stabilizer of 0 in $\mathrm{PSL}_2(\mathbb{Z})$, suppose

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot 0 = \frac{b}{d} = 0 \quad \Rightarrow \quad b = 0.$$

Hence, the stabilizer consists of matrices of the form

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \quad c \in \mathbb{Z},$$

which form a cyclic subgroup generated by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Proposition 5.12. *The matrix*

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

is the image under ϕ of the word $TRT \in F_2$, where

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proof. Direct computation verifies that

$$TRT = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

□

This shows that TRT acts trivially on the untangle.

The kernel $\ker\phi$ consists of elements that act trivially on $\mathbb{Q} \cup \{\infty\}$, i.e., elements that induce the identity Möbius transformation. In $\mathrm{PSL}_2(\mathbb{Z})$, we have the relation:

$$\mathrm{PSL}_2(\mathbb{Z}) = \langle R, T \mid R^2 = \mathrm{id}, (TR)^3 = \mathrm{id} \rangle.$$

Thus, the kernel is normally generated by conjugates of R^2 and $(TR)^3$ in F_2. That is, every element of the kernel is a product of conjugates of these two relations.

Proposition 5.13. *Elements of the form WR^2W^{-1} and $W(TR)^3W^{-1}$ act trivially on all rational tangles.*

Proof. Since τ factors through the quotient $F_2 \to \mathrm{PSL}_2(\mathbb{Z})$, and the images of R^2 and $(TR)^3$ are identity transformations, any conjugate of them acts trivially on τ, hence preserves the isotopy class of the untangle. □

5.3 AM Problem Session

Problem 5.14.

1. *Show that any rotation of the circle is homotopic to the identity map on the circle. Convince yourself (prove!) that there are only two elements of Homeo(S^1) modulo homotopy.*

2. *Describe some homeomorphisms of the torus that are homotopic to the identity. Describe some that are not! Use your knowledge of the homology or fundamental group of the torus to prove that your examples work, or ask a classmate what this means.*

Solution.

1. Let $R_\theta : S^1 \to S^1$ be a rotation by angle θ. A homotopy from R_θ to the identity map id_{S^1} is given by the family of maps $H : S^1 \times [0,1] \to S^1$ defined by $H(z,t) = R_{(1-t)\theta}(z)$. This is a continuous map with $H(z,0) = R_\theta(z)$ and $H(z,1) = z$, so all rotations are homotopic to the identity.

   The group $\pi_0(\mathrm{Homeo}(S^1))$ classifies homeomorphisms up to isotopy, which for manifolds is equivalent to homotopy. Homeomorphisms of the circle are classified by their degree, which can be either $+1$ (orientation-preserving) or -1 (orientation-reversing). Any orientation-preserving homeomorphism is homotopic to a rotation, and thus to the identity. Any orientation-reversing homeomorphism (e.g., complex conjugation $z \mapsto \bar{z}$ on the unit circle) is homotopic to any other orientation-reversing homeomorphism. Since homotopy is an equivalence relation and preserves orientation, the two classes are distinct. Therefore, $\pi_0(\mathrm{Homeo}(S^1))$ consists of two elements.

2. For the torus $T^2 = S^1 \times S^1$, any homeomorphism that is homotopic to the identity must induce the identity map on all homotopy invariants, such as the fundamental group and homology groups. A homeomorphism supported on a small disk (one that is the identity outside the disk) is an example of a map homotopic to the identity.

   A Dehn twist, T_α, about a non-separating simple closed curve α is a canonical example of a homeomorphism not homotopic to the identity. Let α be the meridian $S^1 \times \{\mathrm{pt}\}$ and β be the longitude $\{\mathrm{pt}\} \times S^1$. These curves represent a basis for the first homology group, $H_1(T^2, \mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}$. The action of the Dehn twist T_α on this homology group is given by the matrix representation $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ with respect to the basis $\{[\beta], [\alpha]\}$. Since this is not the identity matrix, the map T_α is not homotopic to the identity map.

□

Problem 5.15. *Describe the inverse of a Dehn twist. How might you prove that it's the inverse?*

Solution. The inverse of a Dehn twist T_α about a simple closed curve α is a Dehn twist about the same curve but in the opposite direction, denoted T_α^{-1}. If T_α is defined by a "right-handed" (e.g., counter-clockwise) twist of 360° in an annular neighborhood of α, then T_α^{-1} is defined by a "left-handed" (clockwise) twist of 360°.

To prove that T_α^{-1} is the inverse of T_α, one must show that their composition is isotopic to the identity map. The homeomorphisms T_α and T_α^{-1} are supported on the same annular neighborhood of α. Let's consider the effect of the composition on this annulus. The first map, T_α^{-1}, introduces a full clockwise twist. The second map, T_α, applies a full counter-clockwise twist. The net effect is that any curve crossing the annulus is first twisted one way and then precisely untwisted back to its original configuration. This composite deformation, which is the identity on the boundary of the annulus, can be continuously unwound back to the identity map via an isotopy that is fixed outside the annulus. Thus, the composition $T_\alpha \circ T_\alpha^{-1}$ is isotopic to the identity, establishing that one is the inverse of the other. □

Problem 5.16. *Show that there is a simple closed curve α in the Klein bottle that does not admit a neighborhood homeomorphic to a cylinder/annulus. (This may be taken as the definition of non-orientability of the surface.) Explain why this meshes with our definition of a Dehn twist about α.*

Solution. The Klein bottle K can be constructed from a square by identifying the edges according to the gluing relation $aba^{-1}b$. Consider the simple closed curve α that runs along the center line corresponding to the identified edges a. This curve is a one-sided curve within the surface. Any tubular neighborhood of this curve is homeomorphic to a Möbius strip, not to an annulus (a cylinder). An annulus is an orientable surface with two distinct boundary components. A Möbius strip is a non-orientable surface with only one boundary component.

The standard definition of a Dehn twist requires an annular neighborhood of the curve α. The construction involves fixing one boundary component (cuff) of the annulus while twisting the other. Since the neighborhood of the curve α in the Klein bottle is a Möbius strip, which possesses only a single boundary component, there are no two distinct cuffs to twist relative to each other. Consequently, a Dehn twist as defined for orientable surfaces cannot be performed along this one-sided curve. This illustrates that the concept of a Dehn twist is fundamentally tied to two-sided curves, which always have annular neighborhoods, a property guaranteed in orientable surfaces.

□

Problem 5.17.

1. *The classification of compact orientable surfaces with boundary says that two such connected surfaces are homeomorphic if and only if they have the same number of boundary components and the same genus. Use this to prove that if S is a compact orientable surface and $\alpha \subset S$ is a non-separating simple closed curve (so that $S \backslash \alpha$ is connected), and β is any other non-separating simple closed curve, then there is a homeomorphism $f : S \to S$ such that $f(\alpha) = \beta$.*

2. *Prove that any two pairs of simple closed curves that intersect once can be taken to each other by an orientation-preserving homeomorphism of the surface.*

Solution.

1. This is a fundamental result known as the "change of coordinates principle" for mapping class groups. Let S be a compact, orientable surface, and let α be a non-separating simple closed curve. Cutting S along α results in a new connected surface, S', with two boundary components, which we can label α_1 and α_2. The classification of surfaces with boundary states that such surfaces are uniquely determined up to homeomorphism by their genus and number of boundary components. Let β be another non-separating simple closed curve on S. Cutting S along β yields a surface S'' which also has two boundary components and the same genus as S'. By the classification theorem, S' and S'' must be homeomorphic. Let $h : S' \to S''$ be such a homeomorphism. We can construct the desired homeomorphism $f : S \to S$ by ensuring the boundaries are mapped correctly before re-gluing. The map h sends the boundary of S' to the boundary of S''. We can choose h such that it maps the boundary component α_1 to β_1 and α_2 to β_2. By identifying the boundaries of S' and S'' according to these maps (which corresponds to reversing the cutting process), the homeomorphism h extends to a homeomorphism $f : S \to S$ that maps the curve α to the curve β.

2. Let (α_1, β_1) and (α_2, β_2) be two pairs of simple closed curves, each with geometric intersection number one. From part (1), we know that since α_1 and α_2 are both non-separating simple closed curves (a curve that intersects another once must be non-separating), there exists a homeomorphism $f_1 : S \to S$ such that $f_1(\alpha_1) = \alpha_2$. Now consider the curve β_1. Its image under f_1 is the curve $f_1(\beta_1)$. Since homeomorphisms preserve intersection numbers, $i(\alpha_2, f_1(\beta_1)) = i(f_1(\alpha_1), f_1(\beta_1)) = i(\alpha_1, \beta_1) = 1$. Both $f_1(\beta_1)$ and β_2 are simple closed curves that intersect the curve α_2 exactly once. We can choose an annular neighborhood of α_2, and within this neighborhood, the curves $f_1(\beta_1)$ and β_2 appear as simple arcs crossing the annulus. There exists a homeomorphism of the surface, f_2, which is supported within this annulus and is the identity on its boundary (thus fixing α_2), that maps the arc of $f_1(\beta_1)$ to the arc of β_2. The composite homeomorphism $f = f_2 \circ f_1$ then has the desired property:

$f(\alpha_1) = f_2(f_1(\alpha_1)) = f_2(\alpha_2) = \alpha_2$, and $f(\beta_1) = f_2(f_1(\beta_1)) = \beta_2$. This demonstrates that the mapping class group acts transitively on the set of isotopy classes of pairs of curves that intersect exactly once.

□

5.4 PM Session 1: Ramanujan's Constant

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field, where $D \in \mathbb{Z}_{>0}$. Define the ring of algebraic integers in K as

$$\mathcal{O}_K = \{x \in K \mid x \text{ is a root of a monic polynomial in } \mathbb{Z}[x]\} \subseteq K.$$

In analogy with the inclusion $\mathbb{Z} \subseteq \mathbb{Q}$, we view $\mathcal{O}_K$ as the integral closure of $\mathbb{Z}$ in K.

Let $E = \mathbb{C}/\Lambda$ be an elliptic curve. The endomorphism ring of E is given by $\mathbb{Z}$ in the generic case, or an order $\mathcal{O} \subseteq \mathcal{O}_K$ if E has CM, where $\mathcal{O}$ is an order in an imaginary quadratic field K and is a rank-2 free $\mathbb{Z}$-module:

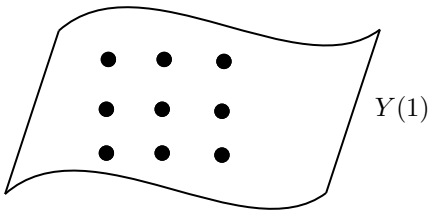
$$\mathbb{Z} \subseteq \mathcal{O} \subseteq \mathcal{O}_K.$$

There is a canonical bijection:

$$\mathrm{Cl}(\mathcal{O}_K) \longrightarrow \{\text{isomorphism classes of elliptic curves } E/\mathbb{C} \text{ with CM by } \mathcal{O}_K\},$$

given explicitly by $[a] \mapsto \mathbb{C}/a$, where $a \subseteq K \subseteq \mathbb{C}$ is a fractional ideal of $\mathcal{O}_K$. Since $\mathrm{Cl}(\mathcal{O}_K)$ is a finite abelian group, the set of isomorphism classes of such elliptic curves is finite.

For each $D \in \mathbb{Z}_{>0}$, we obtain a collection of special points on the modular curve $Y(1)$:



These points correspond to elliptic curves $E/\mathbb{C}$ with complex multiplication by $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, and are referred to as **CM points** on $Y(1)$.

Theorem 5.18 (Duke; Michel-Venkatesh)**.** *Let $D \equiv 1 \pmod 4$. Then the CM points on $Y(1)$ associated to the field $\mathbb{Q}(\sqrt{-D})$ become equidistributed with respect to the Poincaré measure on $Y(1)$ as $D \to \infty$.*

Now we return to discuss

$$e^{\pi\sqrt{163}} \approx 262537412640768743.99999925...$$

is almost an integer.

Sketch of Explanation. We previously defined the modular j-invariant:

$$j : Y(1) \longrightarrow \mathbb{C},$$

and noted that for an elliptic curve $E/\mathbb{C}$ and any $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$, we have:

$$j(E^{\sigma}) = \sigma(j(E)).$$

Suppose E has CM by $\mathcal{O}_K$, and assume $\mathrm{Cl}(\mathcal{O}_K)$ is trivial. Then for all $\sigma \in \mathrm{Aut}(\mathbb{C})$, we must have $\sigma(j(E)) = j(E)$, so $j(E) \in \mathbb{Q}$. In fact, one can prove that $j(E) \in \mathbb{Z}$.

As $\mathrm{Im}(\tau) \to \infty$, we have the classical approximation:

$$j(\tau) \sim e^{-2\pi i\tau}.$$

Now let $K = \mathbb{Q}(\sqrt{-163})$. Since $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$, there exists a unique (up to isomorphism) elliptic curve $E/\mathbb{C}$ with CM by $\mathcal{O}_K$ and $j(E) \in \mathbb{Z}$.

A standard calculation yields that the corresponding CM point is

$$\tau = \frac{1+\sqrt{-163}}{2}.$$

Hence,

$$j\left(\frac{1+\sqrt{-163}}{2}\right) \approx e^{\pi\sqrt{163}}.$$

This explains why $e^{\pi\sqrt{163}}$ is so close to an integer: it is exponentially approximating the integer value of the j-invariant at a CM point. □

5.5 PM Session 2: Rational Tangles II

We consider the following group actions:

(A1) The free group F_2 acts on the set of tangles $\mathcal{T}$: $F_2 \circlearrowright \mathcal{T}$.

(A2) The modular group $\mathrm{PSL}_2(\mathbb{Z}) = \langle R, T \mid R^2, (TR)^3 \rangle$ acts on $\mathbb{Q} \cup \{\infty\}$.

Question: Why should matrices act on tangles?

Answer: Through the theory of braids.

(A3) The braid group B_3 acts on tangles: $B_3 \circlearrowright \mathcal{T}$.

Proposition 5.19. *If τ is a rational tangle and $\beta \in B_3$, then $\beta \cdot \tau$ is also rational.*

Proof. It suffices to check that for $\tau \in \mathcal{T}$, we have $\sigma_1 \cdot \tau, \sigma_2 \cdot \tau \in \mathcal{T}$. □

Proposition 5.20. *The action of B_3 on $\mathcal{T}$ factors through $PSL_2(\mathbb{Z})$:*

$$\begin{array}{lccc} A_3: & B_3 & \curvearrowright & \mathcal{T} \\ & & \searrow & \circlearrowleft \\ & & & PSL_2(\mathbb{Z}) \end{array}$$

under the homomorphism $B_3 \to PSL_2(\mathbb{Z})$ given by

$$\sigma_1 \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \sigma_2 \mapsto \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Proposition 5.21. *The center $Z(B_3)$ is generated by $(\sigma_1\sigma_2\sigma_1)^2 = (\sigma_1\sigma_2)^3$, and we have the isomorphism*

$$B_3/Z(B_3) \cong PSL_2(\mathbb{Z}),$$

realized via the same matrix assignment.

Lemma 5.22. *The actions satisfy $R \cdot_{A1} \tau = (\sigma_1\sigma_2\sigma_1) \cdot_{A3} \tau$.*

Proof of Proposition. We must verify that $Z(B_3) = \langle (\sigma_1\sigma_2\sigma_1)^2 \rangle$ acts trivially on $\mathcal{T}$. But

$$(\sigma_1\sigma_2\sigma_1)^2 \cdot_{A3} \tau = R^2 \cdot_{A1} \tau,$$

and since R^2 acts trivially, so does the center. □

We have seen that

$$B_3 = \pi_1(\mathrm{Conf}_3(\mathbb{C})) = \pi_1(\mathrm{Poly}_3(\mathbb{C})),$$

the fundamental group of the space of monic cubic polynomials with distinct roots.

A map $X \to Y$ induces $\pi_1(X) \to \pi_1(Y)$. In our case, $B_3 \to \mathrm{PSL}_2(\mathbb{Z})$ corresponds to a topological quotient, where

$$\pi_1^{\mathrm{orb}}(\mathbb{H}/\mathrm{PSL}_2(\mathbb{Z})) = \mathrm{PSL}_2(\mathbb{Z}).$$

This motivates viewing $Y(1)$ as the relevant moduli space.

Given $f(x) \in \mathrm{Conf}_3(\mathbb{C})$, the equation $y^2 = f(x)$ defines an elliptic curve of the form $\mathbb{C}/\Lambda$.

This generalizes to higher genus via hyperelliptic curves, but we do not elaborate further.

We recall the presentation $B_3 = \langle x, y \mid x^2 = y^3 \rangle$, and note:

Proposition 5.23. *There is a homotopy equivalence*

$$\mathrm{Conf}_3(\mathbb{C}) \simeq S^3 \backslash \textit{trefoil}.$$

Proof. Consider the subspace $\mathrm{Conf}_3^0(\mathbb{C}) \subseteq \mathrm{Conf}_3(\mathbb{C})$ of depressed cubics. There is a deformation retraction from $\mathrm{Conf}_3(\mathbb{C})$ onto this subspace. □

Define $\mathrm{Conf}_3^0(\mathbb{C}) = \{(a,b) \in \mathbb{C}^2 \mid z^3 + az + b \text{ has 3 distinct roots}\}$. The discriminant is

$$\Delta(a,b) = 4a^3 - 27b^2.$$

Define an action of $\mathbb{C}^\times$ by

$$\lambda \cdot (a,b) = (\lambda^2 a, \lambda^3 b).$$

Proposition 5.24. *The discriminant Δ is invariant under the $\mathbb{C}^\times$-action.*

This allows normalization: given $(a,b) \in \mathrm{Conf}_3^0(\mathbb{C})$, we may rescale so that $\|a\|^2 + \|b\|^2 = 1$, identifying the image with a subset of $S^3 \subseteq \mathbb{C}^2$.

We define

$$S^3 \cap \mathrm{Conf}_3^0(\mathbb{C}) = \{(a,b) \mid 4a^3 \neq 27b^2\} = S^3 \backslash \text{trefoil}.$$

Indeed, the set $\{(a,b) \in \mathbb{C}^2 \mid \|a\|^2 + \|b\|^2 = 2, a^3 = b^2\}$ parametrizes the trefoil knot via the embedding

$$\theta \mapsto \left(e^{2i\theta}, e^{3i\theta}\right), \quad \theta \in S^1,$$

yielding the $(3,2)$ torus knot.

5.6 PM Problem Session

Problem 5.25. *Let G be a group acting on a set X.*

1. *Let $g \in G$ and $x \in X$. Describe the relationship between the stabilizers of x and of $g \cdot x$.*
2. *Let $H \lhd G$ be a normal subgroup that fixes a point $x \in X$. Prove that H fixes the entire orbit of x.*
3. *Let $h, g \in G$ be commuting elements. Prove that the set of fixed points of g, Fix(g), is invariant under the action of h.*
4. *Let A and B be commuting diagonalizable linear transformations on a vector space V. Prove that there exists a basis for V consisting of simultaneous eigenvectors for both A and B.*

Solution.

1. The stabilizers of x and $g \cdot x$ are conjugate. Specifically, the stabilizer of the point $g \cdot x$ is the conjugate of the stabilizer of x by the element g, i.e., $G_{g \cdot x} = gG_x g^{-1}$. To prove this, we show mutual inclusion. First, let $h \in G_{g \cdot x}$. By definition, $h(g \cdot x) = g \cdot x$. Applying the action of g^{-1} to both sides gives $(g^{-1}hg) \cdot x = x$, which shows that $g^{-1}hg \in G_x$. Thus, $h \in gG_x g^{-1}$. Conversely, let $k \in gG_x g^{-1}$. Then $k = ghg^{-1}$ for some $h \in G_x$. We check its action on $g \cdot x$: $k(g \cdot x) = (ghg^{-1})(g \cdot x) = g(h \cdot x) = g \cdot x$. Thus, $k \in G_{g \cdot x}$.

2. Let $x \in X$ be a point fixed by every element of the normal subgroup $H \triangleleft G$. We must show that any other point in the orbit of x, say $y = g \cdot x$ for some $g \in G$, is also fixed by H. Let $h \in H$ be arbitrary. We compute the action of h on y:
$$h \cdot y = h \cdot (g \cdot x) = (hg) \cdot x.$$
Since H is a normal subgroup, there exists an element $h' \in H$ such that $hg = gh'$. Therefore,
$$(hg) \cdot x = (gh') \cdot x = g \cdot (h' \cdot x).$$
By hypothesis, x is fixed by all elements of H, so $h' \cdot x = x$. This gives $g \cdot (h' \cdot x) = g \cdot x = y$. We have shown that $h \cdot y = y$ for all $h \in H$, so the entire orbit of x is fixed by H.

3. Let $h, g \in G$ be such that $hg = gh$. Let $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ be the set of points fixed by g. We want to show that for any $x \in \mathrm{Fix}(g)$, its image $h \cdot x$ is also in $\mathrm{Fix}(g)$. We test this by applying g to the point $h \cdot x$:
$$g \cdot (h \cdot x) = (gh) \cdot x.$$
Using the commutativity of g and h, this becomes:
$$(hg) \cdot x = h \cdot (g \cdot x).$$
Since $x \in \mathrm{Fix}(g)$, we have $g \cdot x = x$. Substituting this gives $h \cdot x$. Thus, we have shown $g \cdot (h \cdot x) = h \cdot x$, which means $h \cdot x$ is a fixed point of g. Therefore, the set $\mathrm{Fix}(g)$ is invariant under the action of h.

4. Let A and B be commuting, diagonalizable linear operators on a vector space V. For any eigenvalue λ of A, let $V_\lambda = \ker(A - \lambda I)$ be the corresponding eigenspace. We first show that V_λ is an invariant subspace under the action of B. Let $v \in V_\lambda$. Then $Av = \lambda v$. We apply A to the vector Bv:
$$A(Bv) = (AB)v = (BA)v = B(Av) = B(\lambda v) = \lambda(Bv).$$
This shows that Bv is also an eigenvector of A with eigenvalue λ, so $Bv \in V_\lambda$. Thus, $B(V_\lambda) \subseteq V_\lambda$.

   Since B is diagonalizable on the entire space V, its restriction to any invariant subspace, such as $B|_{V_\lambda}$, must also be diagonalizable. This means

that the eigenspace V_λ admits a basis consisting of eigenvectors of B. Let this basis be $\{v_1, \ldots, v_k\}$. Each of these vectors is, by construction, an eigenvector of B. Furthermore, since every vector in V_λ is an eigenvector of A with eigenvalue λ, each v_i is also an eigenvector of A. Therefore, $\{v_1, \ldots, v_k\}$ is a basis of simultaneous eigenvectors for A and B within the subspace V_λ.

Since V is the direct sum of the eigenspaces of A, $V = \bigoplus_\lambda V_\lambda$, we can construct a basis for the entire space V by taking the union of the bases of simultaneous eigenvectors from each eigenspace. This proves the existence of a basis for V in which both A and B are diagonal.

□

Problem 5.26.

1. *Prove that a complex polynomial $f(z)$ has a repeated root if and only if $f(z)$ shares a root with its derivative $f'(z)$.*
2. *Describe the condition for the quadratic polynomial $az^2 + bz + c$ to have a repeated root.*
3. *Show that $f(z) = z^3 + az + b$ has a repeated root if and only if $4a^3 + 27b^2 = 0$.*

Solution.

1. A polynomial $f(z)$ has a repeated root at z_0 if and only if $(z - z_0)^k$ is a factor of $f(z)$ for some integer $k \geqslant 2$. First, assume $f(z)$ has a repeated root at z_0. Then we can write $f(z) = (z - z_0)^k g(z)$ with $k \geqslant 2$ and $g(z_0) \neq 0$. The derivative is $f'(z) = k(z - z_0)^{k-1} g(z) + (z - z_0)^k g'(z)$. Since $k \geqslant 2$, the exponent $k - 1 \geqslant 1$, so both terms in the sum are divisible by $(z - z_0)$. Thus, $f'(z_0) = 0$, and z_0 is a common root of $f(z)$ and $f'(z)$. Conversely, assume z_0 is a common root, so $f(z_0) = 0$ and $f'(z_0) = 0$. Since $f(z_0) = 0$, we can write $f(z) = (z - z_0)h(z)$ for some polynomial $h(z)$. Differentiating gives $f'(z) = h(z) + (z - z_0)h'(z)$. Evaluating at z_0 gives $f'(z_0) = h(z_0) + 0$. Since $f'(z_0) = 0$, we must have $h(z_0) = 0$. This means $(z - z_0)$ is a factor of $h(z)$, so $h(z) = (z - z_0)j(z)$ for some polynomial $j(z)$. Substituting back gives $f(z) = (z - z_0)^2 j(z)$, which shows that z_0 is a repeated root of $f(z)$.
2. For the quadratic polynomial $f(z) = az^2 + bz + c$, its derivative is $f'(z) = 2az + b$. A repeated root must be a common root of these two polynomials. The only root of the derivative is $z_0 = -b/(2a)$ (assuming $a \neq 0$). For this to be a repeated root, it must also be a root of the original polynomial. We substitute this value into $f(z) = 0$:

$$a\left(-\frac{b}{2a}\right)^2 + b\left(-\frac{b}{2a}\right) + c = 0 \implies a\frac{b^2}{4a^2} - \frac{b^2}{2a} + c = 0.$$

This simplifies to $\frac{b^2}{4a} - \frac{2b^2}{4a} + \frac{4ac}{4a} = 0$, which gives the condition $-b^2 + 4ac = 0$, or $b^2 - 4ac = 0$. This is the familiar discriminant condition.

3. For the depressed cubic $f(z) = z^3 + az + b$, the derivative is $f'(z) = 3z^2 + a$. For a repeated root, there must be a z_0 such that both $f(z_0) = 0$ and $f'(z_0) = 0$. From the derivative, $3z_0^2 + a = 0$, which implies $z_0^2 = -a/3$. From the original polynomial, we have $z_0^3 + az_0 + b = 0$, which can be rewritten as $z_0(z_0^2) + az_0 + b = 0$. Substituting the expression for z_0^2 gives:

$$z_0\left(-\frac{a}{3}\right) + az_0 + b = 0 \implies \frac{2a}{3}z_0 + b = 0.$$

This yields $z_0 = -3b/(2a)$. Now we have two expressions for quantities involving z_0: $z_0^2 = -a/3$ and $z_0 = -3b/(2a)$. Squaring the second expression and equating it with the first gives:

$$\left(-\frac{3b}{2a}\right)^2 = -\frac{a}{3} \implies \frac{9b^2}{4a^2} = -\frac{a}{3}.$$

Cross-multiplying gives $27b^2 = -4a^3$, which is the condition $4a^3 + 27b^2 = 0$. This expression is the discriminant of the depressed cubic polynomial.

□

Problem 5.27.

1. *Let $Poly_k$ be the vector space of complex polynomials of degree at most k. Given fixed polynomials $P \in Poly_m$ and $Q \in Poly_n$, show that the map $M : Poly_{n-1} \times Poly_{m-1} \to Poly_{m+n-1}$ defined by $M(A, B) = AP + BQ$ is linear.*

2. *What is the dimension of $Poly_k$? And of $Poly_m \times Poly_n$?*

3. *Prove that P and Q have a common root if and only if the map M from part (1) is non-invertible.*

4. *By choosing suitable bases, write down the matrix for the map M in the case where $P = az^2 + bz + c$ and $Q = P' = 2az + b$, and compute its determinant.*

5. *Describe a procedure for finding the discriminant of a general polynomial of degree n.*

Solution.

1. The map $M : \text{Poly}_{n-1} \times \text{Poly}_{m-1} \to \text{Poly}_{m+n-1}$ is defined by $(A, B) \mapsto AP + BQ$. To check linearity, we take two pairs (A_1, B_1) and (A_2, B_2) from the domain and a scalar $c \in \mathbb{C}$. $M(c(A_1, B_1) + (A_2, B_2)) = M(cA_1 + A_2, cB_1 + B_2) = (cA_1 + A_2)P + (cB_1 + B_2)Q$. By distributivity of polynomial multiplication, this is $c(A_1P) + A_2P + c(B_1Q) + B_2Q = c(A_1P + B_1Q) + (A_2P + B_2Q) = cM(A_1, B_1) + M(A_2, B_2)$. The map is linear.

2. The vector space Poly_k of polynomials of degree at most k has a basis $\{1, z, \ldots, z^k\}$, so its dimension is $k+1$. The dimension of the product space $\mathrm{Poly}_m \times \mathrm{Poly}_n$ is the sum of the dimensions, $(m+1)+(n+1) = m+n+2$.

3. The map $M : \mathrm{Poly}_{n-1} \times \mathrm{Poly}_{m-1} \to \mathrm{Poly}_{m+n-1}$ is a linear map between two vector spaces of the same dimension, $(n-1+1)+(m-1+1) = n+m$ and $(m+n-1+1) = m+n$. Such a map is non-invertible if and only if it has a non-trivial kernel. Suppose P and Q have a common root z_0. Then $P(z) = (z-z_0)P_1(z)$ and $Q(z) = (z-z_0)Q_1(z)$, where $\deg P_1 = m-1$ and $\deg Q_1 = n-1$. Consider the non-zero pair $(A, B) = (Q_1, -P_1) \in \mathrm{Poly}_{n-1} \times \mathrm{Poly}_{m-1}$. Then $M(A, B) = Q_1P - P_1Q = Q_1(z - z_0)P_1 - P_1(z - z_0)Q_1 = 0$. Thus, the kernel is non-trivial, and M is non-invertible. Conversely, suppose M is non-invertible. Then there exists a non-zero pair (A, B) such that $AP+BQ = 0$, or $AP = -BQ$. Since $\mathbb{C}[z]$ is a unique factorization domain and $\deg A \leqslant n - 1 < \deg Q$, this implies that Q must share an irreducible factor (and thus a root) with P.

4. Let $P = az^2+bz+c$ $(m = 2)$ and $Q = 2az+b$ $(n = 1)$. We consider the map $M : \mathrm{Poly}_0 \times \mathrm{Poly}_1 \to \mathrm{Poly}_2$. A basis for the domain is $\{(1, 0), (0, 1), (0, z)\}$. A basis for the codomain is $\{1, z, z^2\}$.

   - $M(1, 0) = 1 \cdot P + 0 \cdot Q = c + bz + az^2 \implies (c, b, a)$
   - $M(0, 1) = 0 \cdot P + 1 \cdot Q = b + 2az \implies (b, 2a, 0)$
   - $M(0, z) = 0 \cdot P + z \cdot Q = bz + 2az^2 \implies (0, b, 2a)$

   The matrix representation of M is formed by these column vectors:

$$\begin{pmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{pmatrix}.$$

   Its determinant is the resultant of P and Q: $\det(M) = c(4a^2 - 0) - b(2ab - 0) + 0 = 4a^2c - 2ab^2$. This is not the standard discriminant. The standard Sylvester matrix construction yields a slightly different matrix for the system. Let's set up the system correctly: we seek $A(z) = A_0$ and $B(z) = B_1z + B_0$ such that $A_0(az^2 + bz + c) + (B_1z + B_0)(2az + b) = 0$. This gives the linear system in (A_0, B_1, B_0):

$$\begin{aligned} z^2 : &\quad aA_0 + 2aB_1 = 0 \\ z^1 : &\quad bA_0 + bB_1 + 2aB_0 = 0 \\ z^0 : &\quad cA_0 + bB_0 = 0 \end{aligned}$$

   The matrix of coefficients is $\begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix}$. Its determinant is $a(b^2) - 2a(b^2 - 2ac) = -ab^2 + 4a^2c = a(4ac - b^2)$. For a non-trivial solution to exist, this determinant must be zero. Since $a \neq 0$, this is the condition $b^2 - 4ac = 0$.

5. The discriminant of a polynomial P of degree n, denoted $\mathrm{Disc}(P)$, is a polynomial in the coefficients of P that is zero if and only if P has a repeated root. From part (1), this is equivalent to P and its derivative P' having a common root. From part (3), this is equivalent to the non-invertibility of the linear map $M_{P,P',n-1,n-1}$. This non-invertibility is equivalent to the vanishing of the determinant of the matrix representation of this map. This determinant is called the resultant, $\mathrm{Res}(P, P')$. The procedure is therefore: Given $P(z)$, calculate its derivative $P'(z)$. Construct the Sylvester matrix for the linear map $(A, B) \mapsto AP + BP'$ for polynomials A and B of appropriate degree. The discriminant is, up to a sign and a factor depending on the leading coefficient, the determinant of this Sylvester matrix.

□

Problem 5.28. *Let $F(x, y) = 0$ define a curve in $\mathbb{C}^2$. The link of the singularity at zero is its intersection with a small sphere $||x||^2 + ||y||^2 = \epsilon^2$.*

1. *Describe the link of $x^p + y^q = 0$. Is it always a knot?*
2. *Can you find a link that gives you a knot different from anything found in part (a)?*
3. *Can you find a link that gives you the figure-8 knot?*

Solution.

1. The link of the singularity $x^p + y^q = 0$ is the intersection of the algebraic variety $V = \{(x, y) \in \mathbb{C}^2 \mid x^p + y^q = 0\}$ with the 3-sphere $S^3 \subset \mathbb{C}^2$. The resulting space $L_{p,q} = V \cap S^3$ is a link in S^3. To analyze its structure, let $d = \gcd(p, q)$, with $p = da$ and $q = db$ for coprime integers a, b. The equation can be written as $(x^a)^d = (-y^b)^d$. This splits into d components in $\mathbb{C}^2$, each given by $x^a = \zeta_d^k(-y^b)$ for $k = 0, \ldots, d-1$, where ζ_d is a primitive d-th root of unity. Each of these components, when intersected with the 3-sphere, gives a torus knot of type (a, b). Therefore, the link $L_{p,q}$ consists of $d = \gcd(p, q)$ parallel copies of the (a, b)-torus knot. The link is a knot (a single component) if and only if $d = 1$, i.e., if p and q are coprime. If $\gcd(p, q) > 1$, it is a multi-component link.
2. I don't know how to do this.
3. I don't know how to do this.

□