Presentations for Linear Groups

A presentation on presentations

Vanderbilt University

Geometric Group Theory Seminar

Nic Brody, UCSC
October 1, 2025

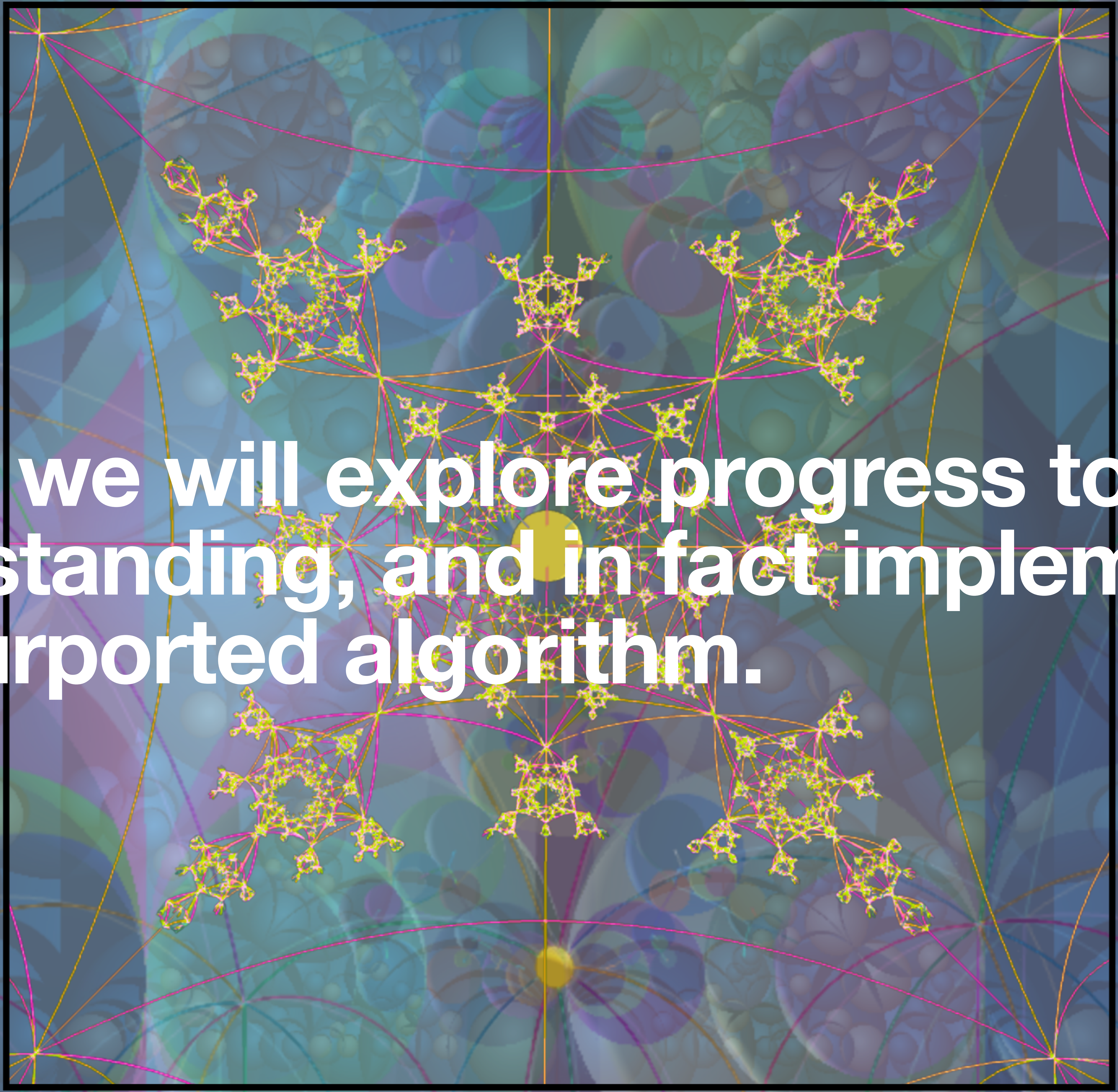
Suppose S is a finite set of invertible two-by-two matrices with algebraic entries.

$$S = \left\{ \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \right\}$$

What is $G = \langle S \rangle$?

Conjecture:

There is an algorithm which takes in a finite set $S \subseteq \mathrm{PGL}_2(\overline{\mathbb{Q}})$, and outputs a presentation for $\langle S \rangle$.



Today, we will explore progress towards understanding, and in fact implementing this purported algorithm.

Suppose k is a number field, and $\mathbb{G}$ is a simple k-algebraic group
We call a subgroup $\Gamma \leq \mathbb{G}(k)$

Suppose k is a number field, and $\mathbb{G}$ is a simple k-algebraic group
We call a subgroup $\Gamma \leq \mathbb{G}(k)$

- *Algebraic* if there is an algebraic subgroup $\mathbb{H}(\mathbb{Q}) \lneq \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}(k)$ with $\Gamma \leq \mathbb{H}(\mathbb{Q})$

Suppose k is a number field, and $\mathbb{G}$ is a simple k-algebraic group
We call a subgroup $\Gamma \leq \mathbb{G}(k)$

- *Algebraic* if there is an algebraic subgroup $\mathbb{H}(\mathbb{Q}) \lneq \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}(k)$ with $\Gamma \leq \mathbb{H}(\mathbb{Q})$

- *Geometric* if there is a valuation v on k so that $\Gamma \leq \mathbb{G}(k_v)$ is discrete

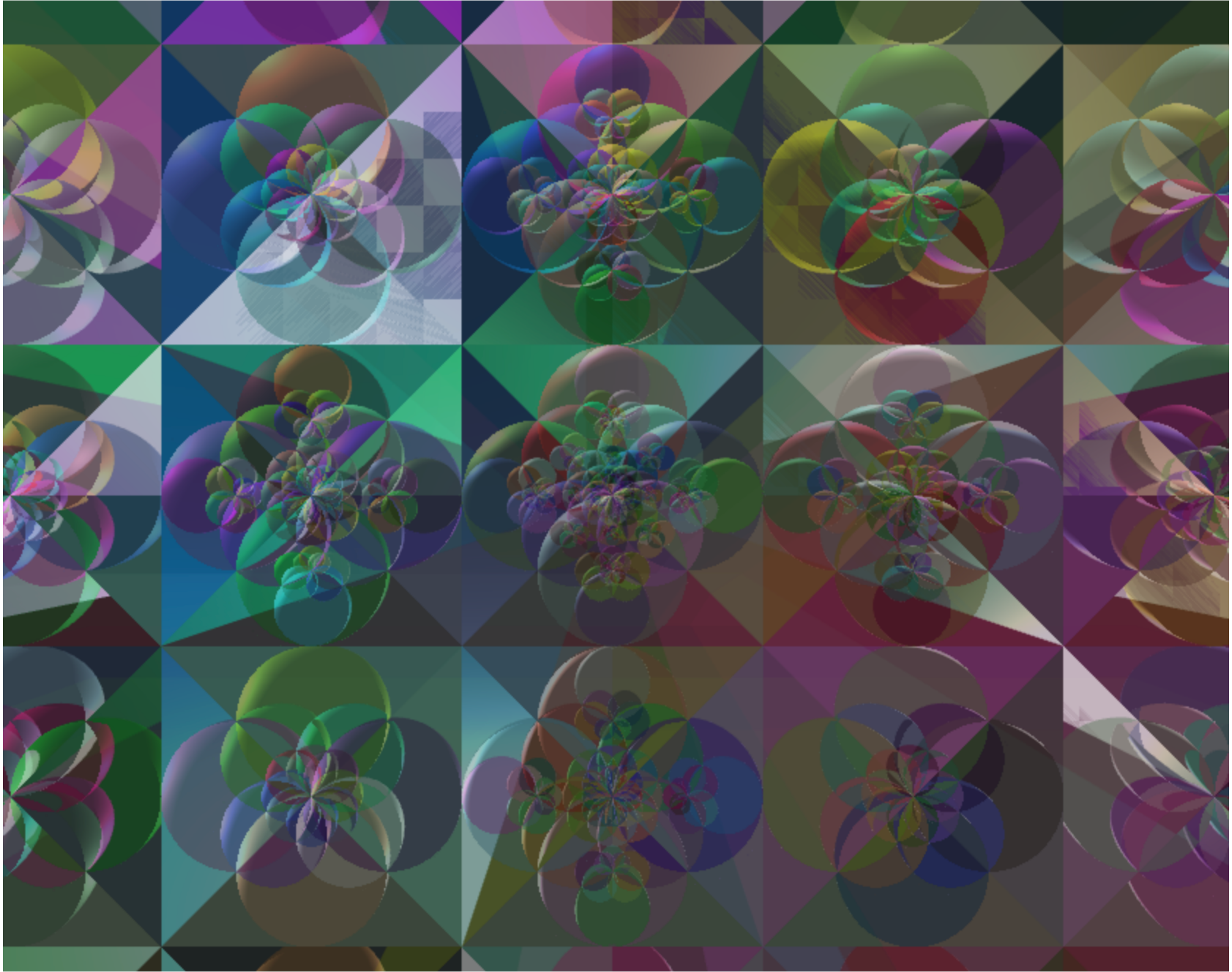
Suppose k is a number field, and $\mathbb{G}$ is a simple k-algebraic group
We call a subgroup $\Gamma \leq \mathbb{G}(k)$

- *Algebraic* if there is an algebraic subgroup $\mathbb{H}(\mathbb{Q}) \lneq \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}(k)$ with $\Gamma \leq \mathbb{H}(\mathbb{Q})$
- *Geometric* if there is a valuation v on k so that $\Gamma \leq \mathbb{G}(k_v)$ is discrete
- *Arithmetic* if there is a subring $A \leq k$ so that Γ is commensurable with $\mathbb{G}(A)$

Suppose k is a number field, and $\mathbb{G}$ is a simple k-algebraic group
We call a subgroup $\Gamma \leq \mathbb{G}(k)$

- *Algebraic* if there is an algebraic subgroup $\mathbb{H}(\mathbb{Q}) \lneq \mathrm{Res}_{k/\mathbb{Q}}\mathbb{G}(k)$ with $\Gamma \leq \mathbb{H}(\mathbb{Q})$
- *Geometric* if there is a valuation v on k so that $\Gamma \leq \mathbb{G}(k_v)$ is discrete
- *Arithmetic* if there is a subring $A \leq k$ so that Γ is commensurable with $\mathbb{G}(A)$

Conj: Every subgroup is one of these!



In the case of $\mathbb{G} = \mathrm{PGL}_2(k)$:

Algebraic subgroups

$$\left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in k \right\} \qquad \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \mid x \in k^* \right\} \qquad \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x \in k^*, y \in k \right\}$$

$$\left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x^2 + y^2 = 1 \right\}$$

$$\left\{ \begin{pmatrix} x & y \\ -\sigma(y) & \sigma(x) \end{pmatrix} \mid x\sigma(x) + y\sigma(y) = 1 \right\}, \sigma \in \mathrm{Gal}(k/\mathbb{Q})$$

In the case of $\mathbb{G} = \mathrm{PGL}_2(k)$:
Geometric subgroups

- Geometric subgroups act properly on:
    - A locally finite tree if v is non-archimedean
    - The hyperbolic plane if $k_v = \mathbb{R}$
    - Hyperbolic 3-space if $k_v = \mathbb{C}$

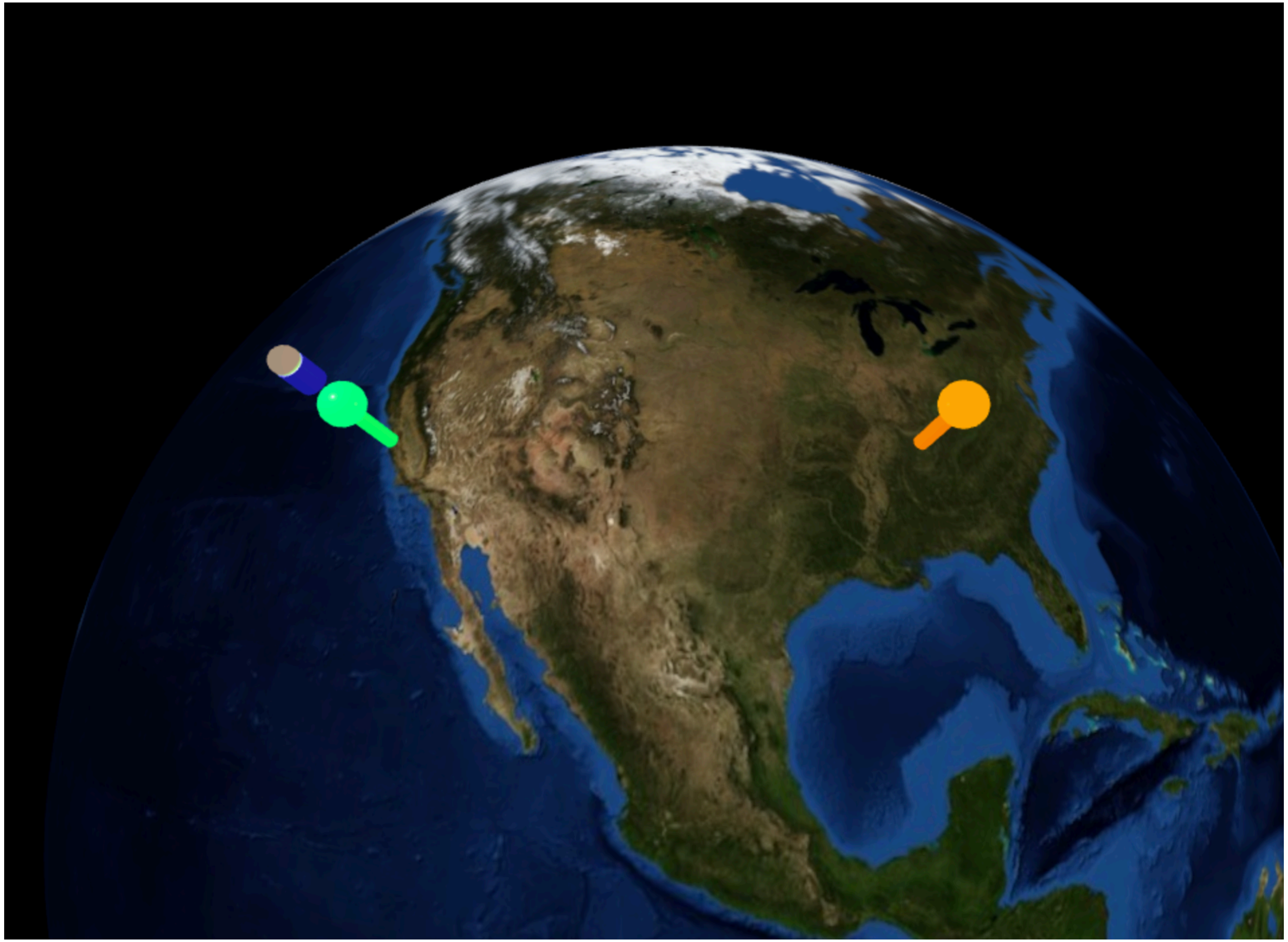
In the case of $\mathbb{G} = \mathrm{PGL}_2(k)$:
Arithmetic subgroups

- Finitely generated subrings of $\overline{\mathbb{Q}}$ embed as a lattice in a finite product of local fields.

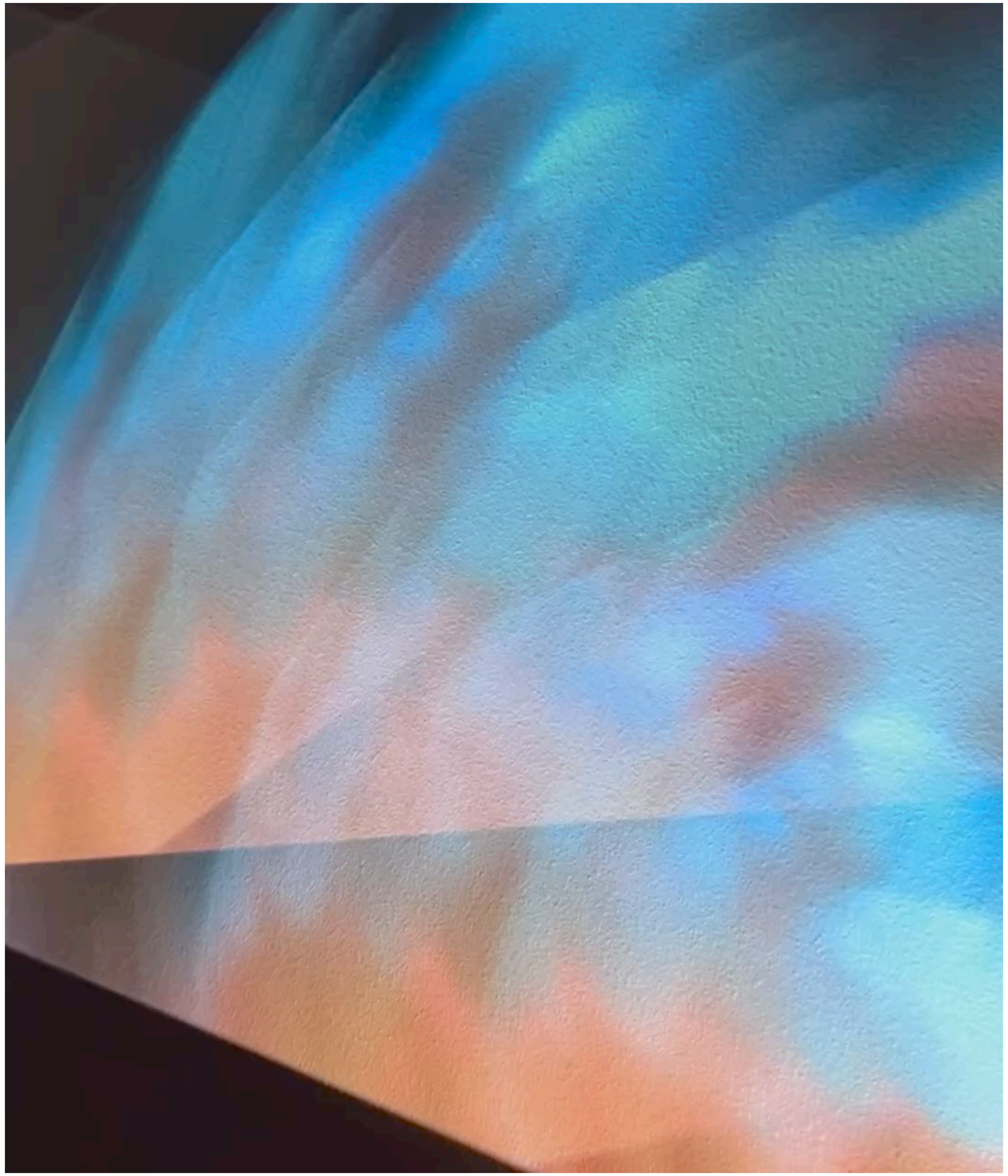
- Consequently, $\mathrm{PGL}_2(A)$ is a lattice in a product of trees, hyperbolic planes, and hyperbolic 3-spaces.

- Unless $A = \mathbb{Z}[\sqrt{-d}]$ or $\mathbb{Z}$, $\mathrm{PGL}_2(A)$ has the *congruence subgroup property*.

Globe game



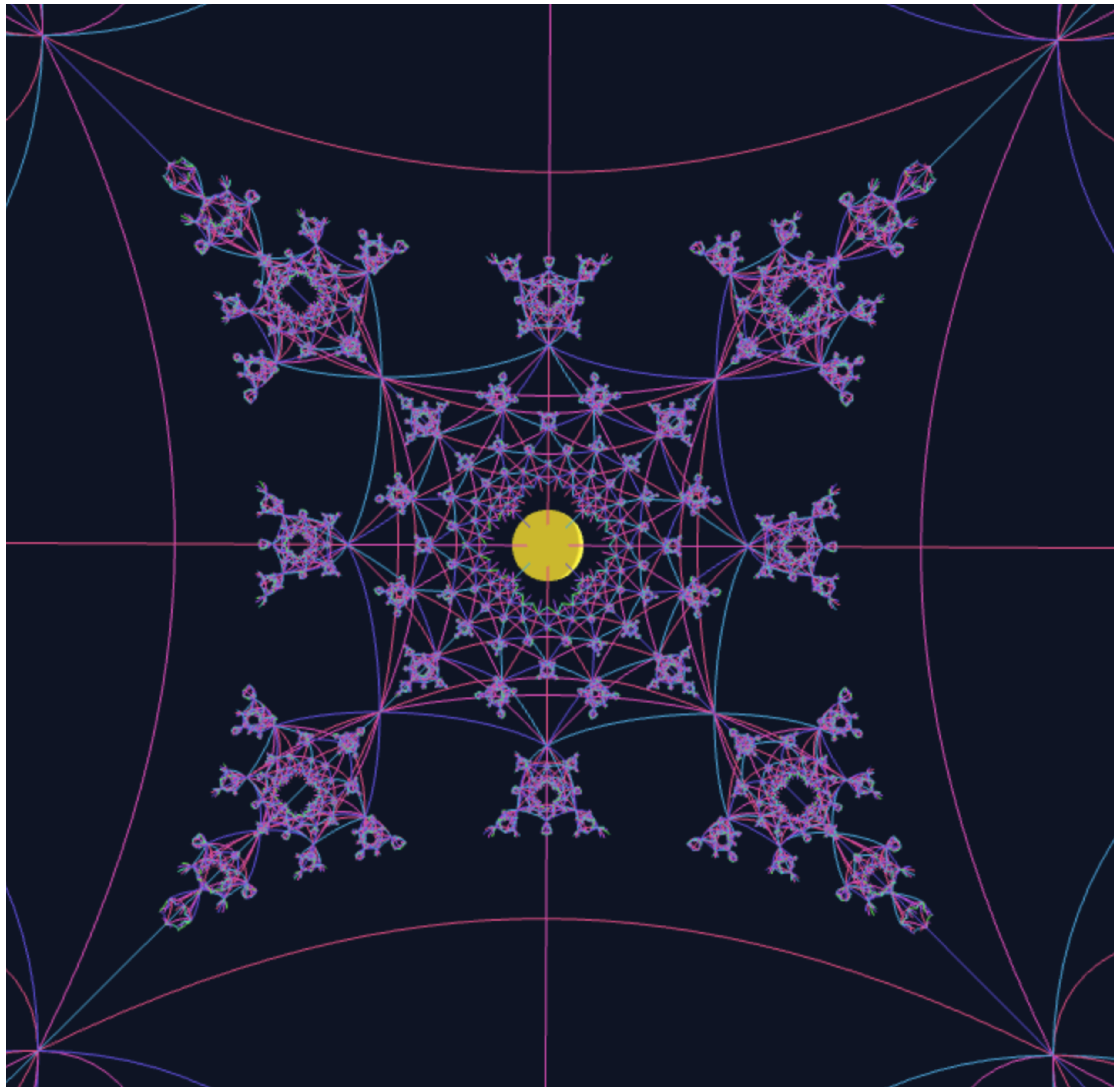
$$\left\langle \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right\rangle$$



Talk outline

- Act 1: Algebraic subgroups
- Act 2: Geometric subgroups
- Act 3: Arithmetic subgroups

Algebraic subgroups



Write $S = \left\{ \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \ldots, \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \right\}$.

The first stage in computing $\langle S \rangle$ is determining the *entry ring*

$$A = \mathbb{Z}[a_i, b_i, c_i, d_i, \frac{1}{a_i d_i - b_i c_i}].$$

This is a finitely generated subring of $\overline{\mathbb{Q}}$; we will call such an object a *number ring.*

Once we have computed the number ring A, Derksen-Jeandal-Koiran provide an algorithm for computing

$$\mathbb{H}(\mathbb{Q}) = \mathrm{Zar}\left(\Gamma \leq \mathrm{Res}_{k/\mathbb{Q}}(\mathbb{G}(k))\right),$$

where $\mathbb{G}$ is any linear algebraic group. For PGL_2, $\mathbb{H}$ is virtually solvable unless it is of unitary type.

$$\mathbb{Z} \leq \mathbb{R}$$

The real line is a connected metric space on which the integers act as isometries. The quotient topological space is the circle S^1, whose fundamental group $\pi_1(S^1) = \mathbb{Z}$.

We would love to mimic this example in greater generality.

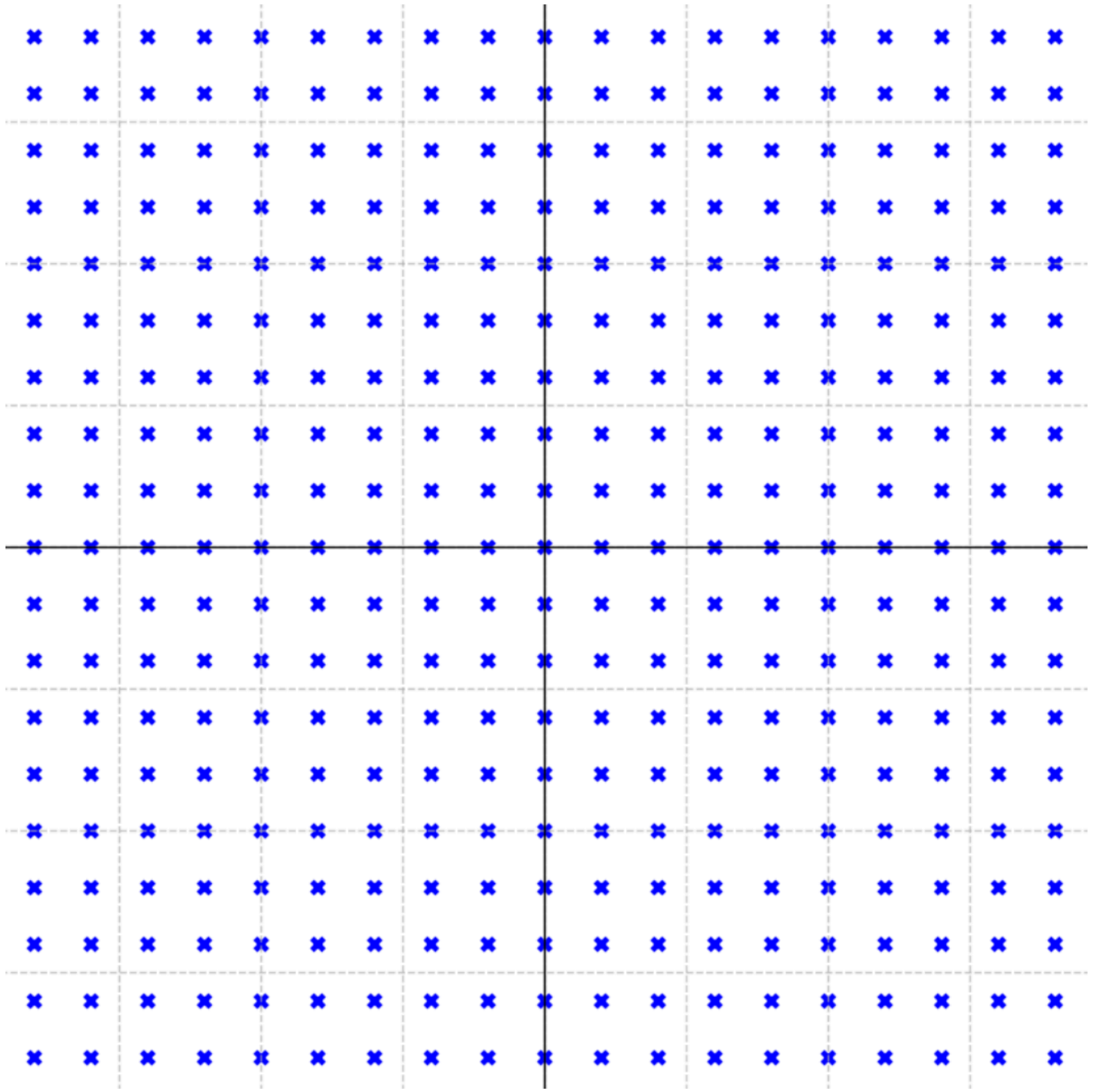
Geometric Group Theory

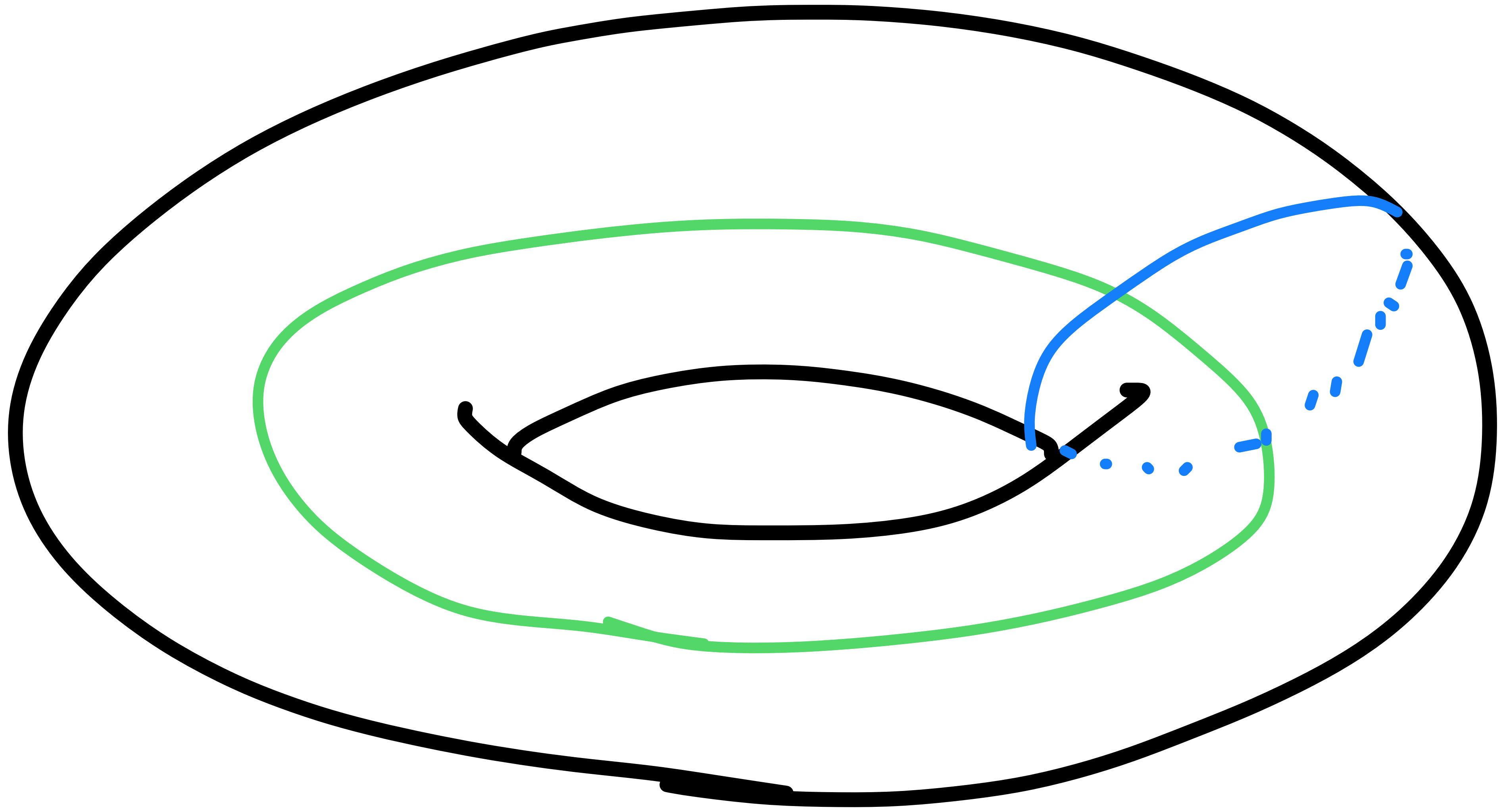
Suppose Γ is a group.

Problem: Find a contractible metric space X, together with a proper isometric action of Γ.

Then $\pi_1^{orb}(X//\Gamma) = \Gamma$

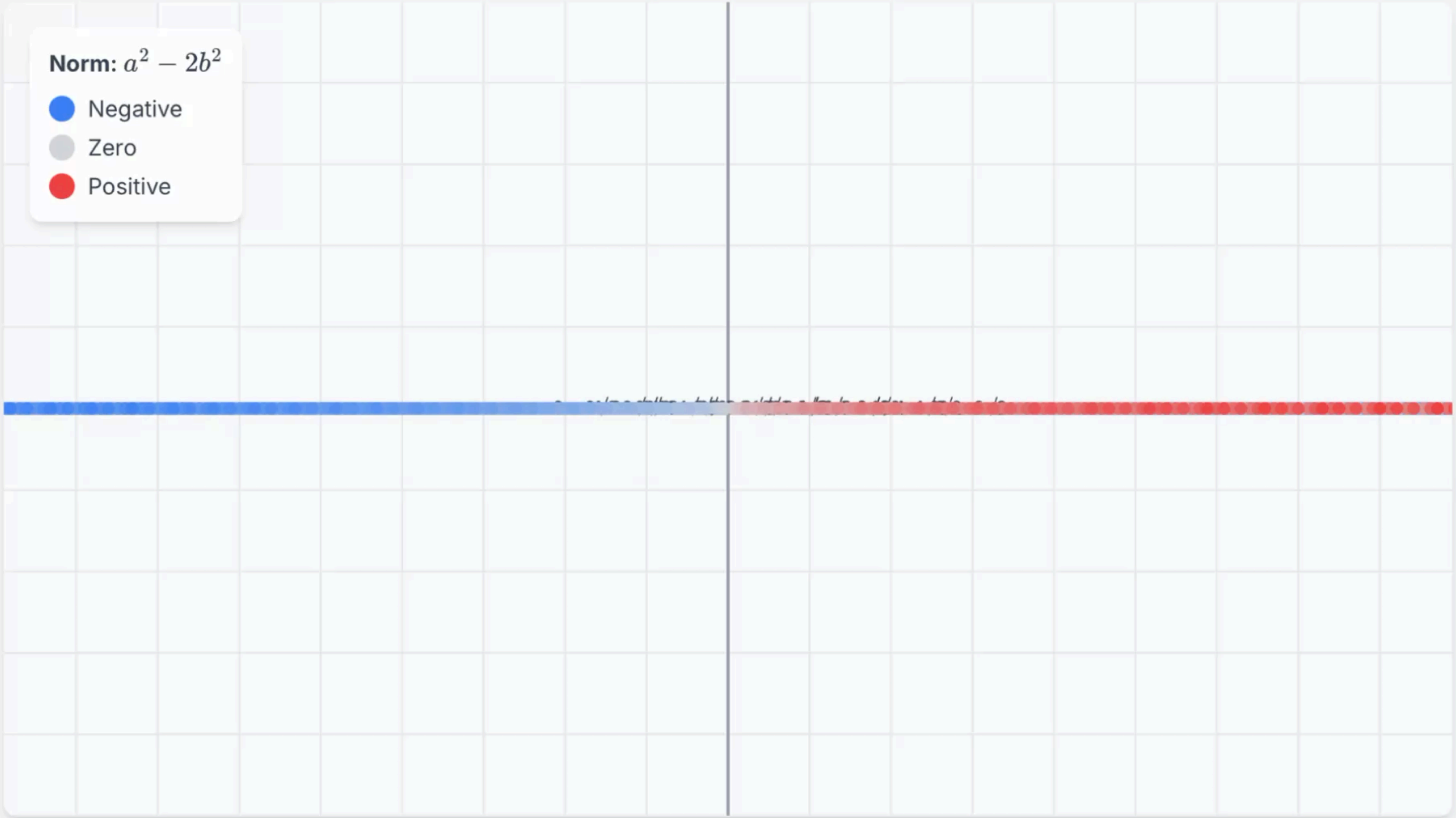
$$\mathbb{Z}[i] \leq \mathbb{C}$$



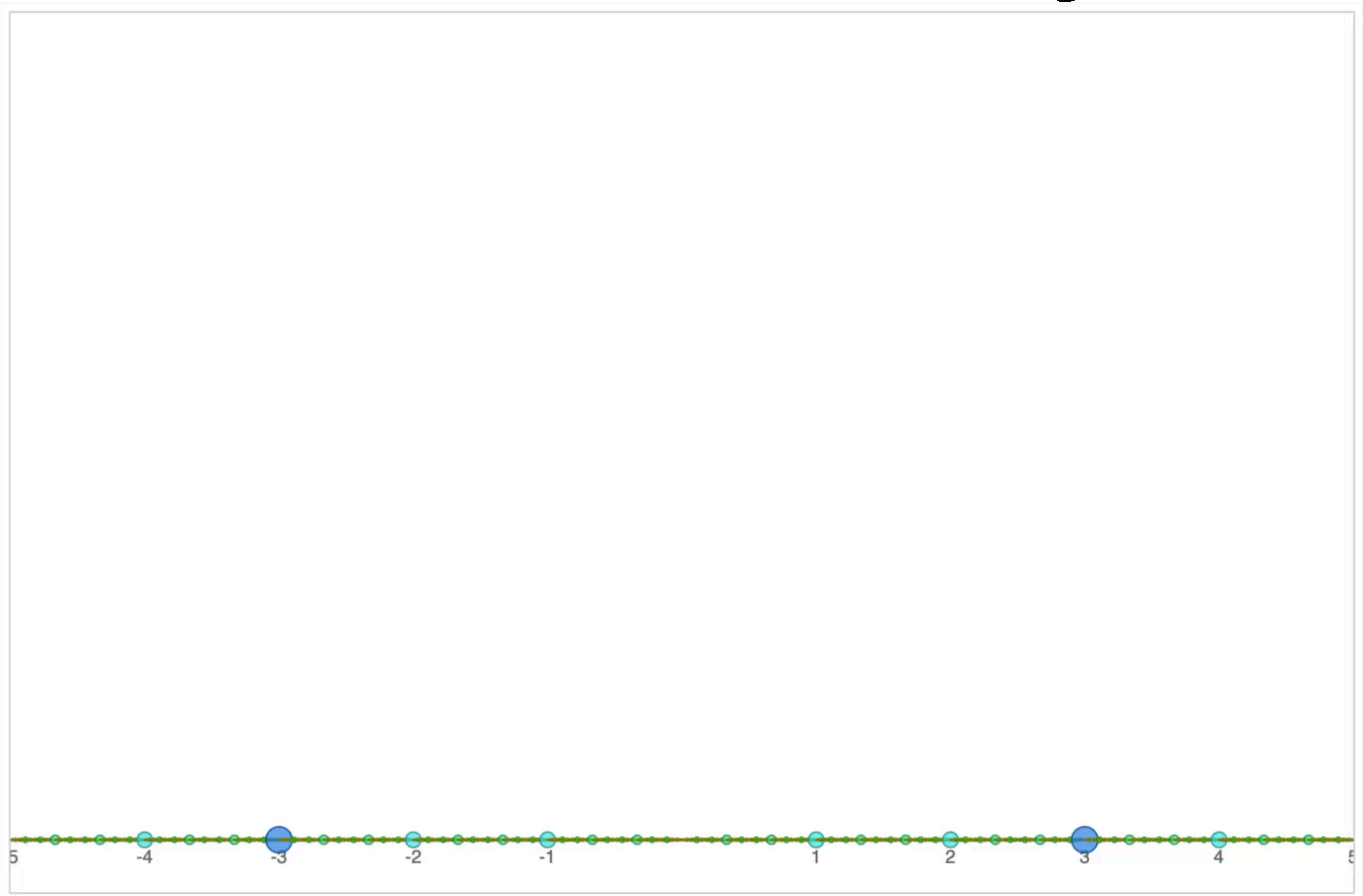


Minkowski Embedding of $\mathbb{Z}[\sqrt{2}]$

Visualizing the mapping from $a + b\sqrt{2}$ to the point $(a + b\sqrt{2},\, a - b\sqrt{2}) \in \mathbb{R}^2$.



$$\mathbb{Z}[1/3] \leq \mathbb{R} \times \mathbb{Q}_3$$



A number ring $A \leq \overline{\mathbb{Q}}$ admits finitely many nontrivial valuations V_A. Moreover,

$$A \leq \prod_{v \in V_A} A_v = \mathbb{A}_A$$

is a lattice, where each A_v is a local field.

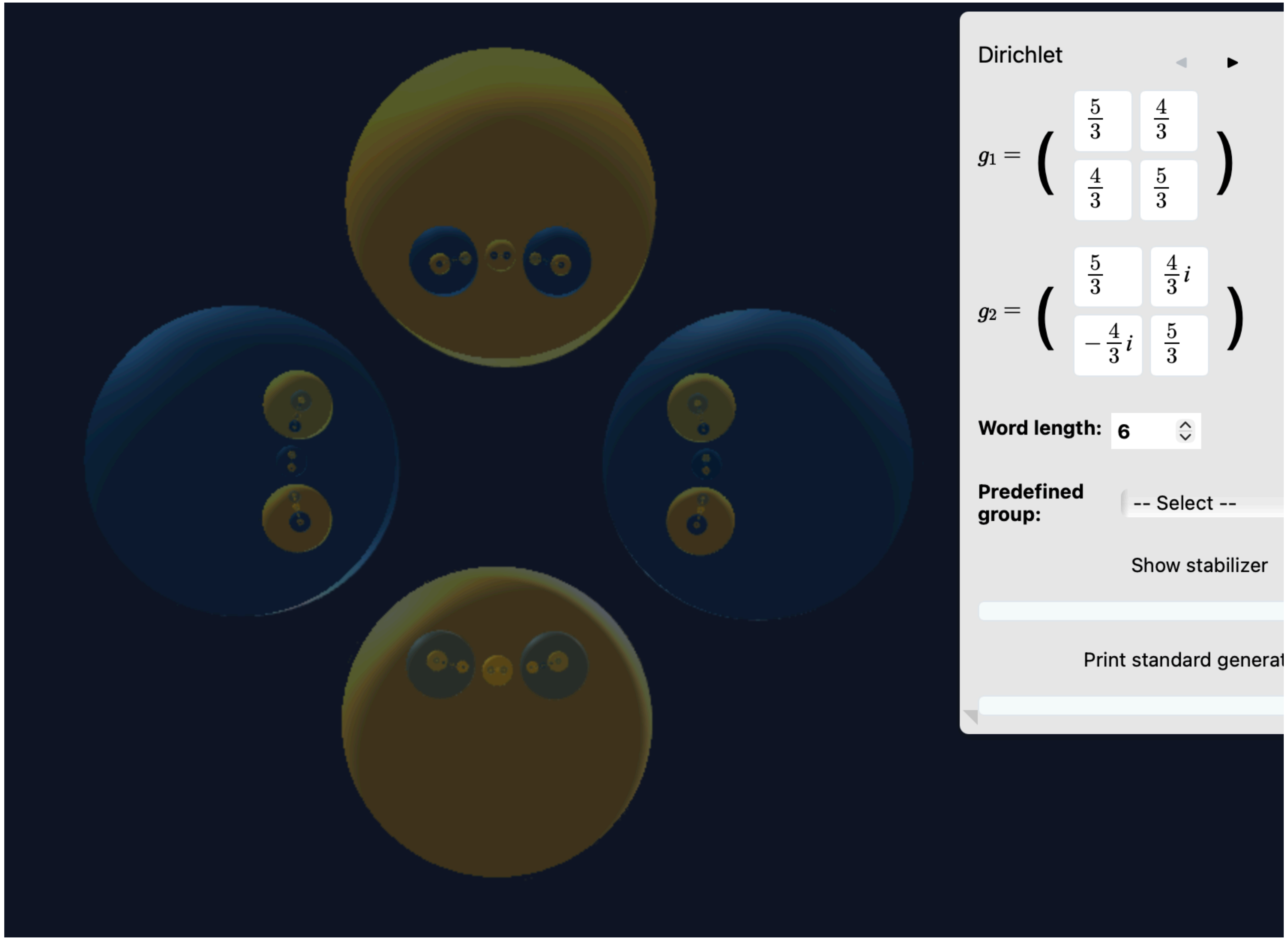
Borel—Harish-Chandra Theorem

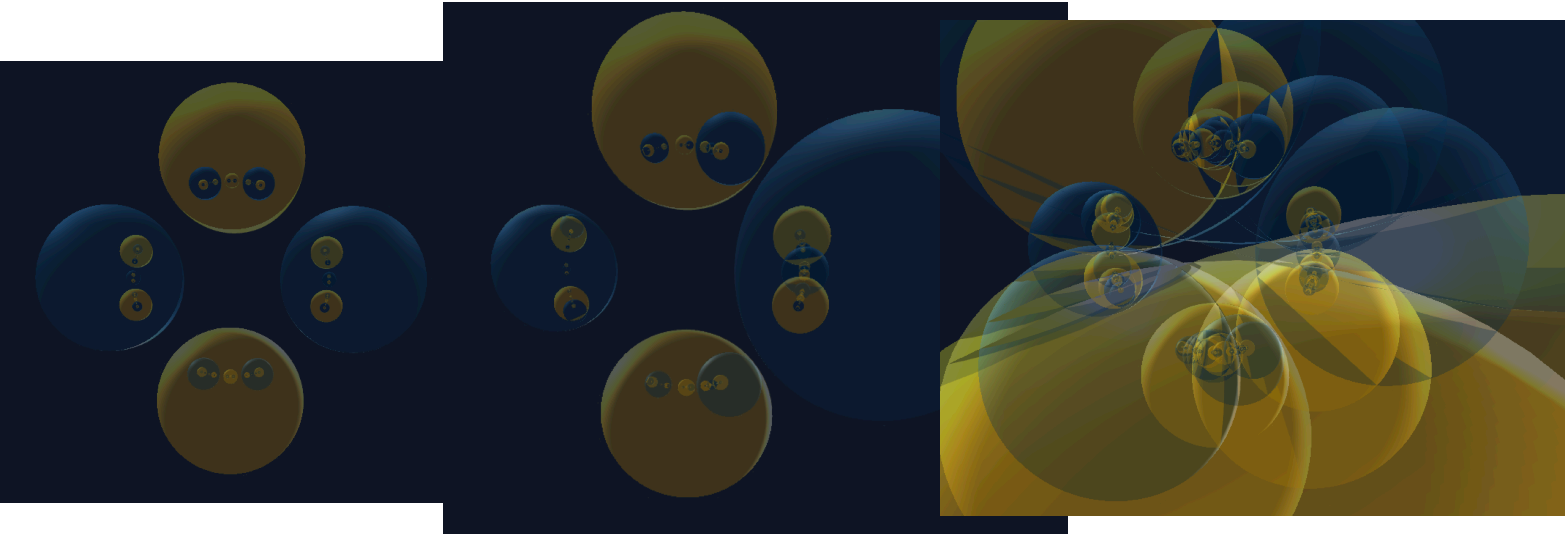
Suppose that A is a number ring, and $\mathbb{G}$ is a semisimple algebraic group.

Then $\mathbb{G}(A)$ is a lattice in $\mathbb{G}(\mathbb{A}_A)$.

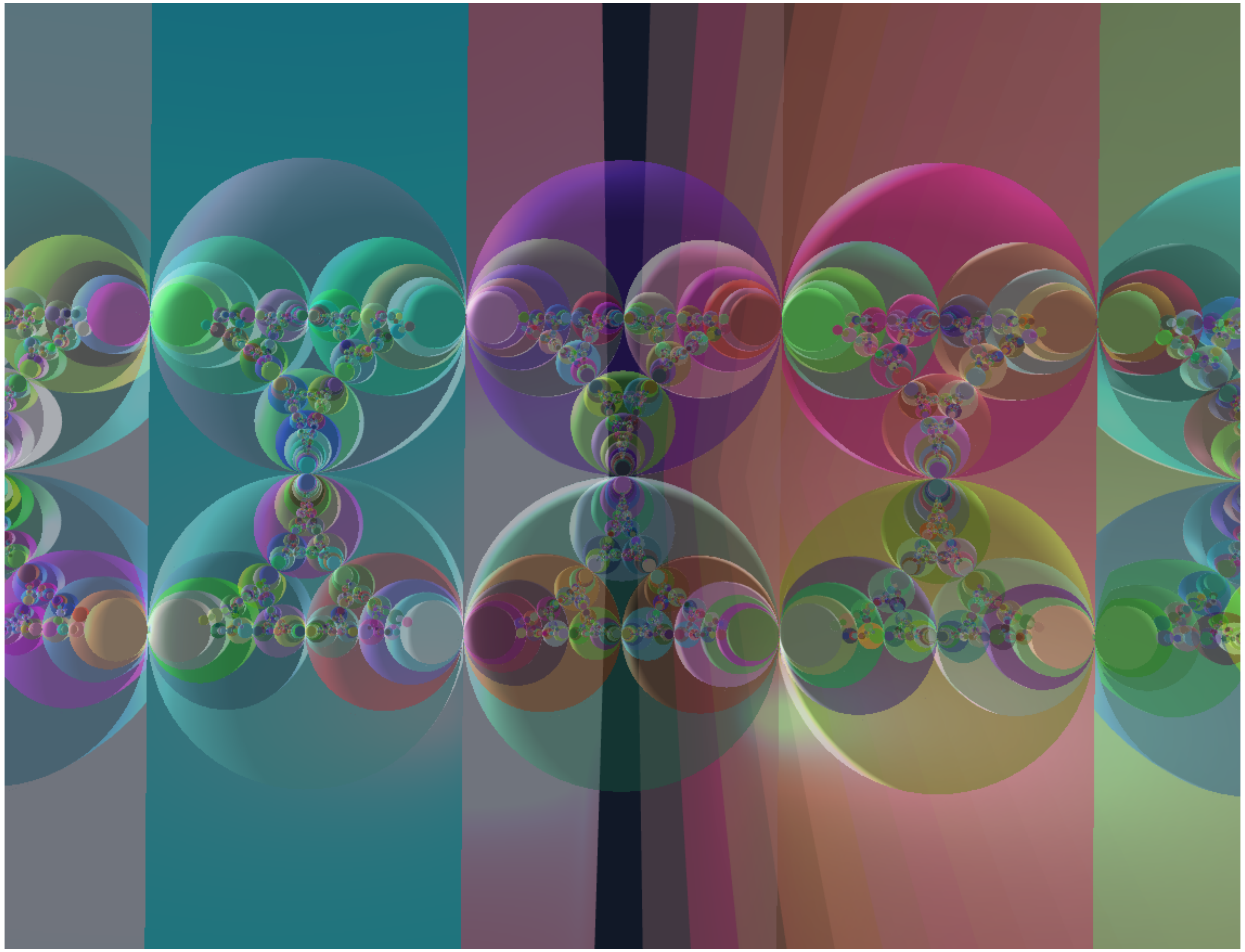
Geometric subgroups

Warm-up: Ping pong





These can often tolerate mild deformations, but it is very possible to bend beyond discreteness! It then becomes difficult to determine the group.



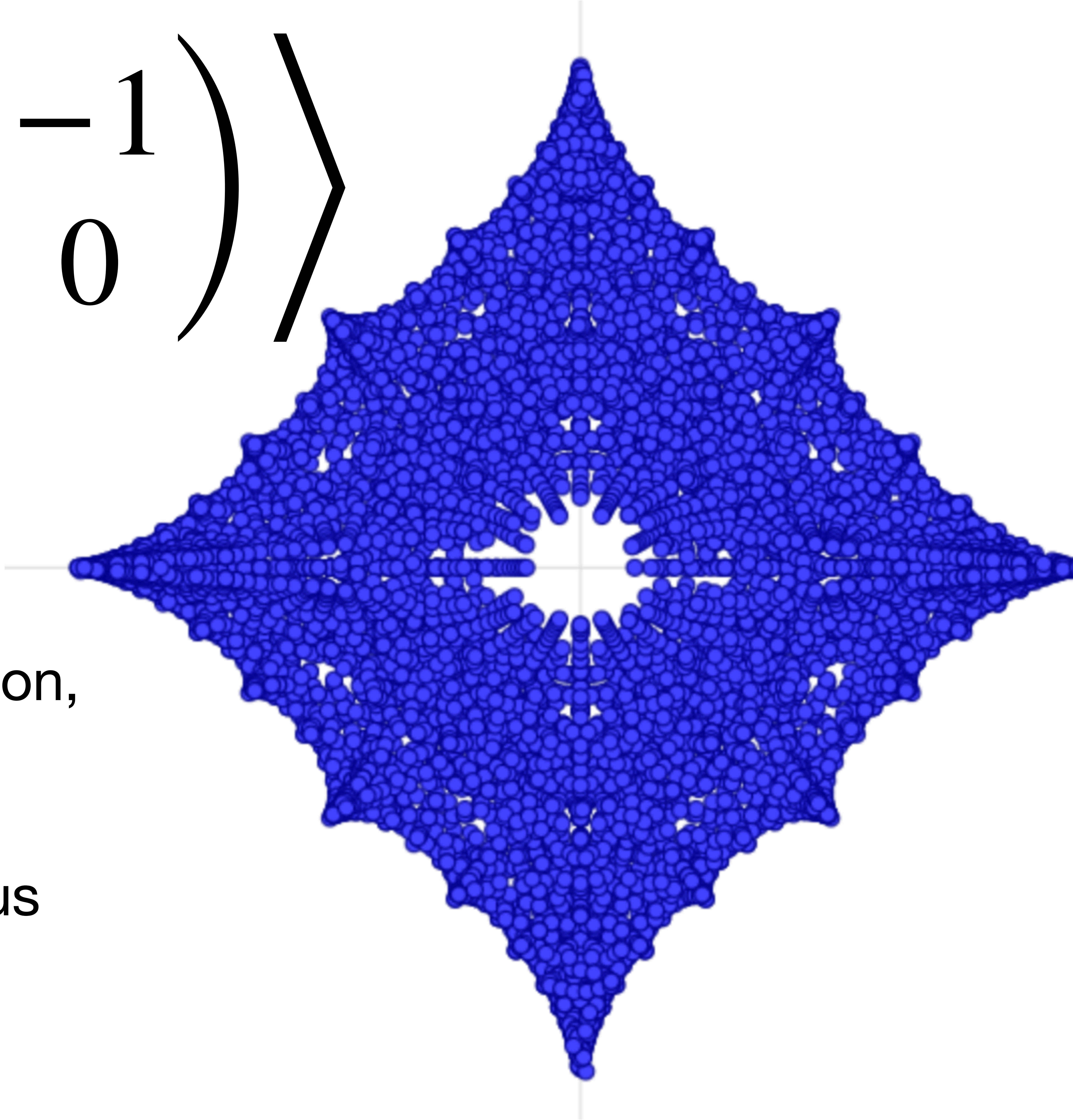
Consider the group

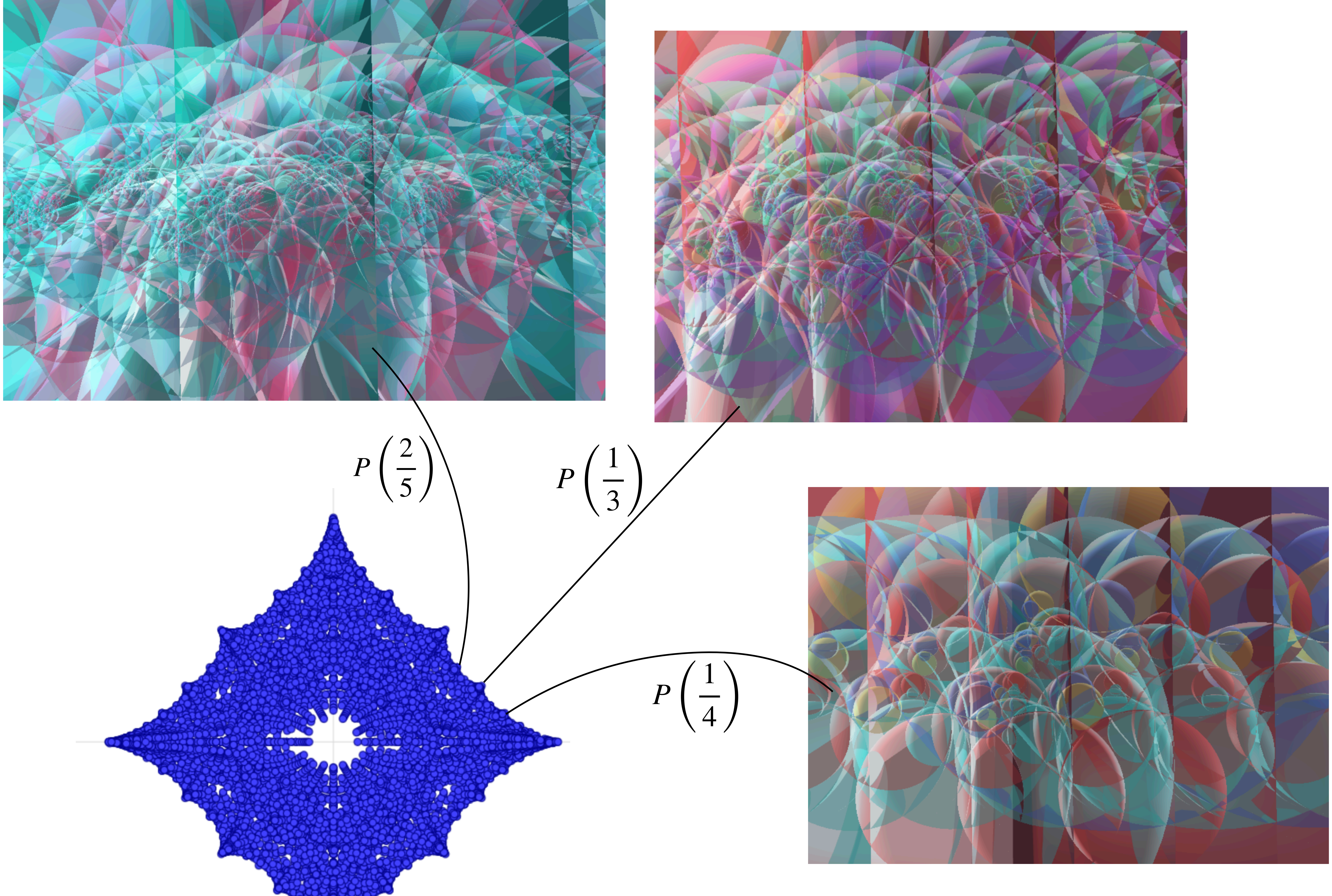
$$\Gamma_z = \left\langle \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

When z is a complex number outside of this region (vertices at $\pm 2, \pm 2i$), the group is discrete and virtually free in $\mathrm{PSL}_2(\mathbb{C})$.

If z has a Galois conjugate outside of this region, then the group is still free (eg, $z = 1 - \sqrt{2}$).

Even though $\Gamma_{1-\sqrt{2}}$ does not have any obvious ping pong sets, its Galois conjugate does!




$P\left(\frac{2}{5}\right)$
$P\left(\frac{1}{3}\right)$
$P\left(\frac{1}{4}\right)$

The classification conjecture implies that Γ_z is $\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ if z has a Galois conjugate in the region, and has finite index in $\mathrm{PSL}_2(\mathbb{Z}[z])$ otherwise.

Recall that a *valuation* on a field determines a metric, and hence endows $\mathbb{G}(k_v)$ with a metric.

We say that a group $\Gamma \leq \mathbb{G}(k)$ is *geometric* if there is a valuation v on k so that Γ is discrete in $\mathbb{G}(k_v)$.

It doesn't make sense to ask whether $\mathrm{SL}_2(\mathbb{Z})$ is discrete in $\mathrm{SL}_2(\mathbb{Q})$; however, upon embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$, we can understand a lot about $\mathrm{SL}_2(\mathbb{Z})$ by studying its action on $\mathrm{SL}_2(\mathbb{R})/\mathbb{SO}_2(\mathbb{R}) = \mathbb{H}^2$.

Now let's consider the group

$$\left\langle \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix}, \frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ 2 & 2 & -1 \end{pmatrix} \right\rangle \leq \mathrm{SO}_3(\mathbb{R})$$

The geometry of $\mathrm{SO}_3(\mathbb{R})$ doesn't provide us with any way to understand the structure of this group.

However, noting that the group is actually contained in $\mathrm{SO}_3(\mathbb{Z}[1/3])$ gives us a clue of what to look for. There is another geometry hidden behind the scenes!

Now let's consider the group

$$\left\langle \frac{1}{3}\begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ -2 & 2 & -1 \end{pmatrix}, \frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ 2 & 2 & -1 \end{pmatrix} \right\rangle \leq \mathrm{SO}_3(\mathbb{R})$$

One can check (by some "residue modulo 3" computations) that any reduced word of length k in these generators will have an entry whose denominator is 3^k. We immediately conclude that this pair of matrices generates a free group. In fact, the group is 3-adically discrete.

These elements play ping pong in the 3-adic tree $\mathrm{SO}_3(\mathbb{Q}_p)/\mathrm{SO}_3(\mathbb{Z}_p)$!

Prime p

3

Inputs

Matrix

3	1/3
0	1

Vertex q

1

Vertex k

1

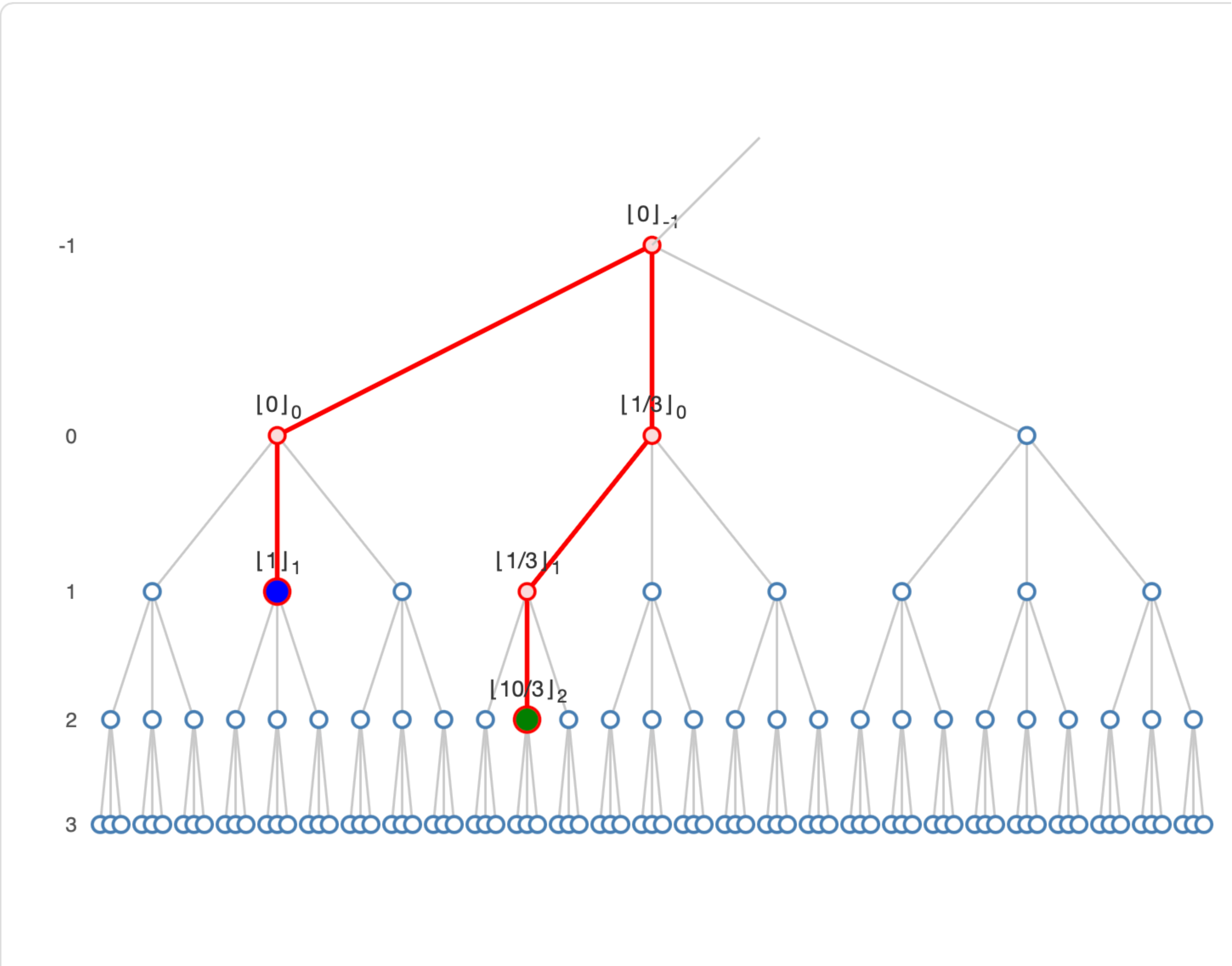
Calculate

Results

Initial Vertex (reduced): $v = \lfloor 1 \rfloor_1$

Resulting Vertex: $a \cdot v = \lfloor 10/3 \rfloor_2$

Distance: $d(v, a \cdot v) = 5$



Canonical Dirichlet Domains

Suppose that $\Gamma \leq \mathrm{O}(n,1;\mathbb{R})$ is a discrete group. Then there is a *canonical* polyhedron $P_\Gamma \leq \mathbb{H}^n$ so that

(1) $\Gamma \cdot P_\Gamma = \mathbb{H}^n$

(2) $\mathrm{Int}(P_\Gamma \cap \gamma P_\Gamma) \neq \emptyset \Rightarrow \gamma = id$.

Canonical Dirichlet Domains

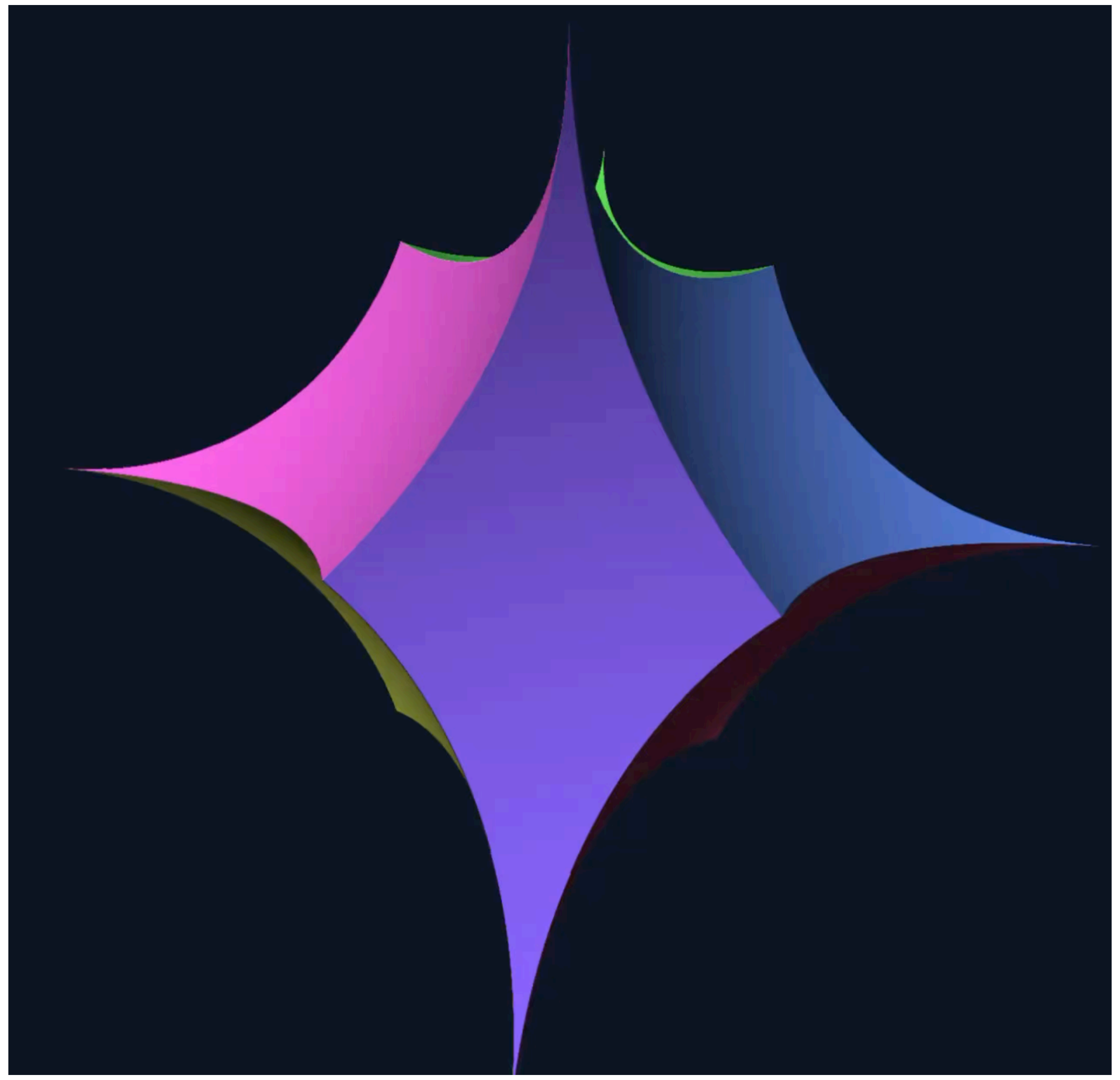
Suppose that $\Gamma \leq \mathrm{O}(n,1;\mathbb{R})$ is a discrete group. Then there is a *canonical* polyhedron $P_\Gamma \leq \mathbb{H}^n$ so that

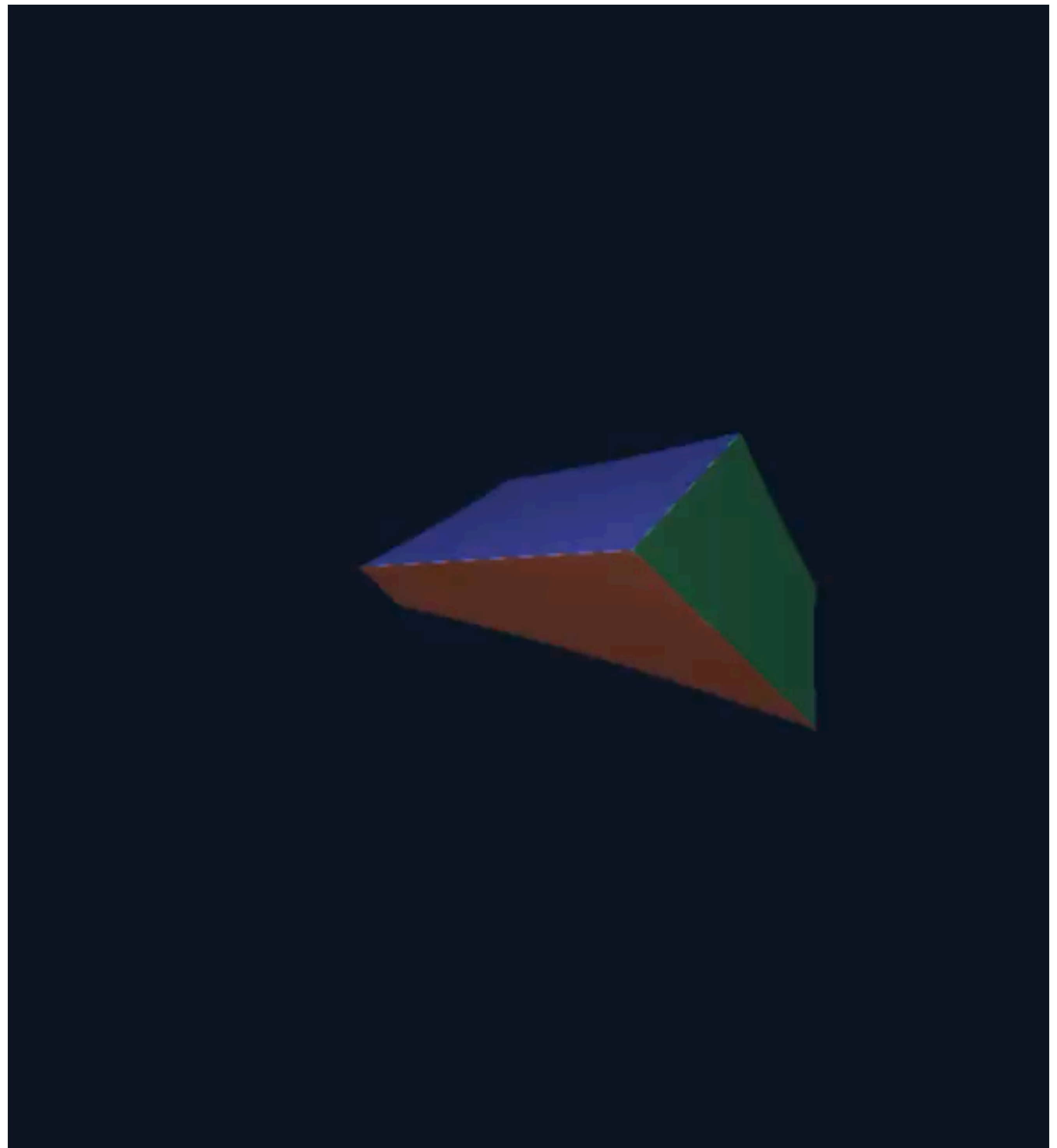
(1) $\Gamma \cdot P_\Gamma = \mathbb{H}^n$

(2) $\mathrm{Int}(P_\Gamma \cap \gamma P_\Gamma) \neq \emptyset \Rightarrow \gamma = id$.

Proof: Take Q_Γ to be the Voronoi cell in $\mathbb{H}^n$ defined by e_{n+1}. Then intersect Q_Γ with the sector determined by $\Gamma \cap \mathrm{O}(n)$, determined inductively by Voronoi cells of the orbit of e_k in $\mathrm{O}(k)$

(The observation is that the "ordered basis" information inherent to $\mathrm{O}(n,1;\mathbb{R})$ gives a natural choice of domain)



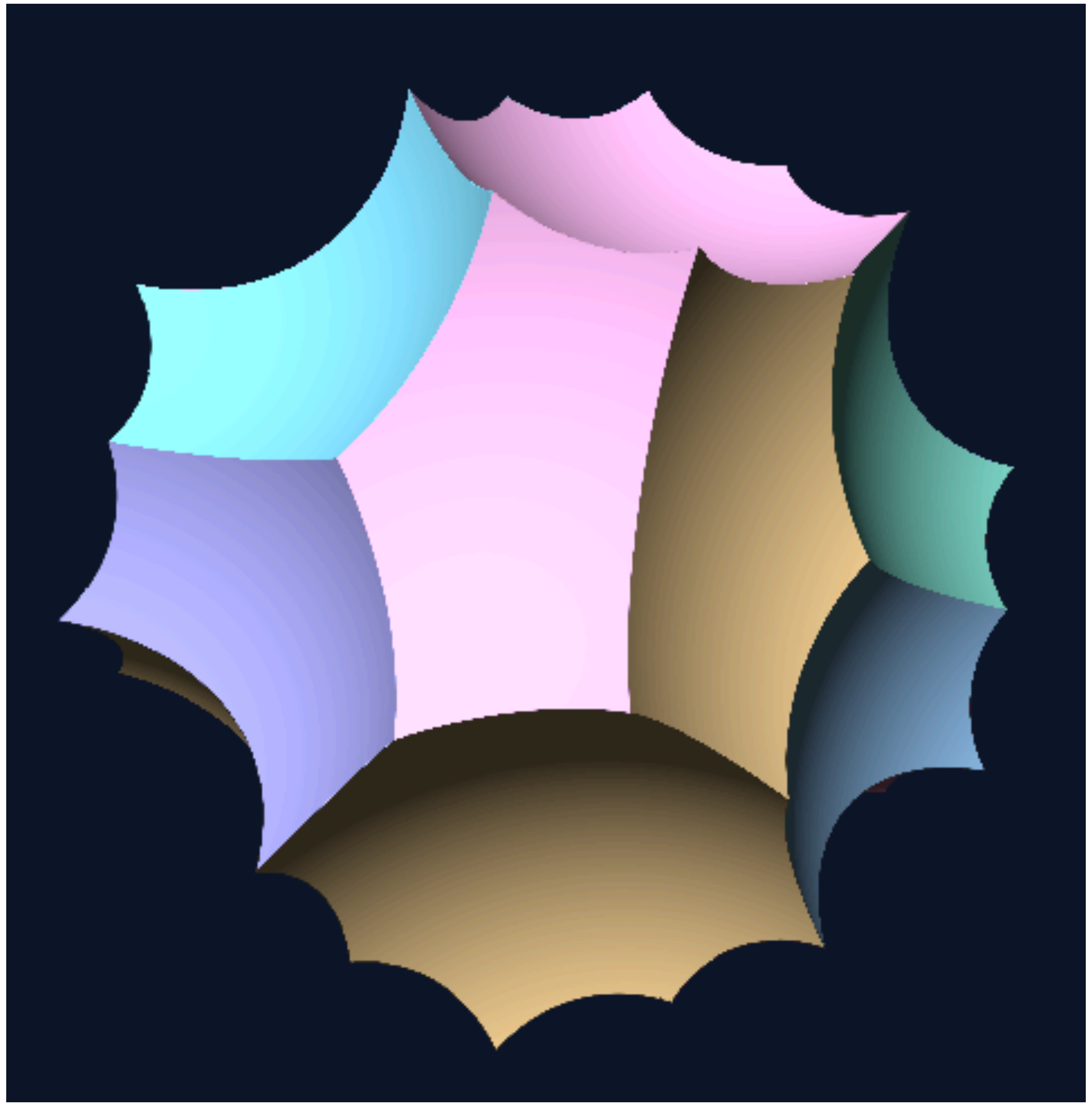



Now, we consider

$$T = \{\gamma \in \Gamma \mid \mathrm{codim}(P_\Gamma \cap \gamma P_\Gamma) = 1\}$$

This set generates Γ, and is finite exactly when Γ is geometrically finite. We call this the *standard generating set*.

Poincaré Polyhedron Theorem



Suppose P is a polyhedron in $\mathbb{H}^3$, together with a collection of face-pairings T.

We say that (P, T) *satisfies the Poincaré Polyhedron Theorem* if each edge cycle is a spherical 1-orbifold.

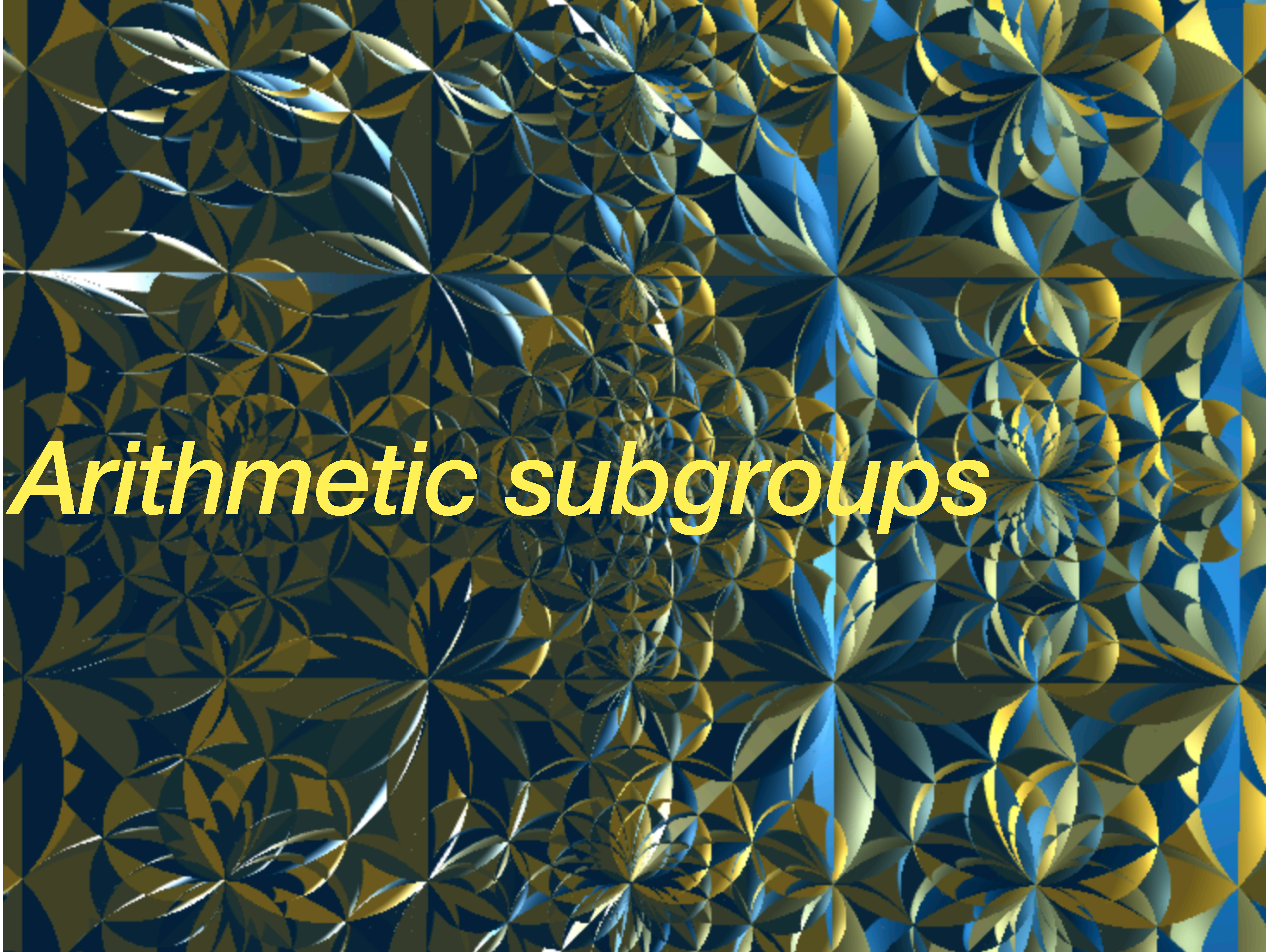
A pair (P, T) satisfying the Poincaré Polyhedron Theorem generates a discrete group.

So, given $S \subseteq \mathrm{PSL}_2(\mathbb{C}) = \mathrm{Isom}(\mathbb{H}^3)$ which generates a discrete group, can we describe an algorithm to compute T?

So, given $S \subseteq \mathrm{PSL}_2(\mathbb{C}) = \mathrm{Isom}(\mathbb{H}^3)$ which generates a discrete group, can we describe an algorithm to compute T?

M. Kapovich proves that this problem is undecidable. However, the proof relies on Baire category arguments, and so it does not apply in the case that the group is contained in $\mathrm{PSL}_2(\overline{\mathbb{Q}})$!

Arithmetic subgroups



Often, when $\Gamma \leq \mathbb{G}(A)$ fails to be discrete in any particular place, we can show that it has *finite index!*

Theorem (B.): If $\mathrm{SO}_3(\mathbb{Z}[1/p]) \leq \Gamma \leq \mathrm{SO}_3(\mathbb{Q})$, then $\Gamma \sim \mathrm{SO}_3(A)$ for a subring $A \leq \mathbb{Q}$

Theorem (Venkataramana): If $\mathbb{G}(\mathbb{R})$ has positive rank and $\mathbb{G}(\mathbb{Z}) \leq \Gamma \leq \mathbb{G}(k)$, then $\Gamma \sim \mathbb{G}(A)$ for some A.

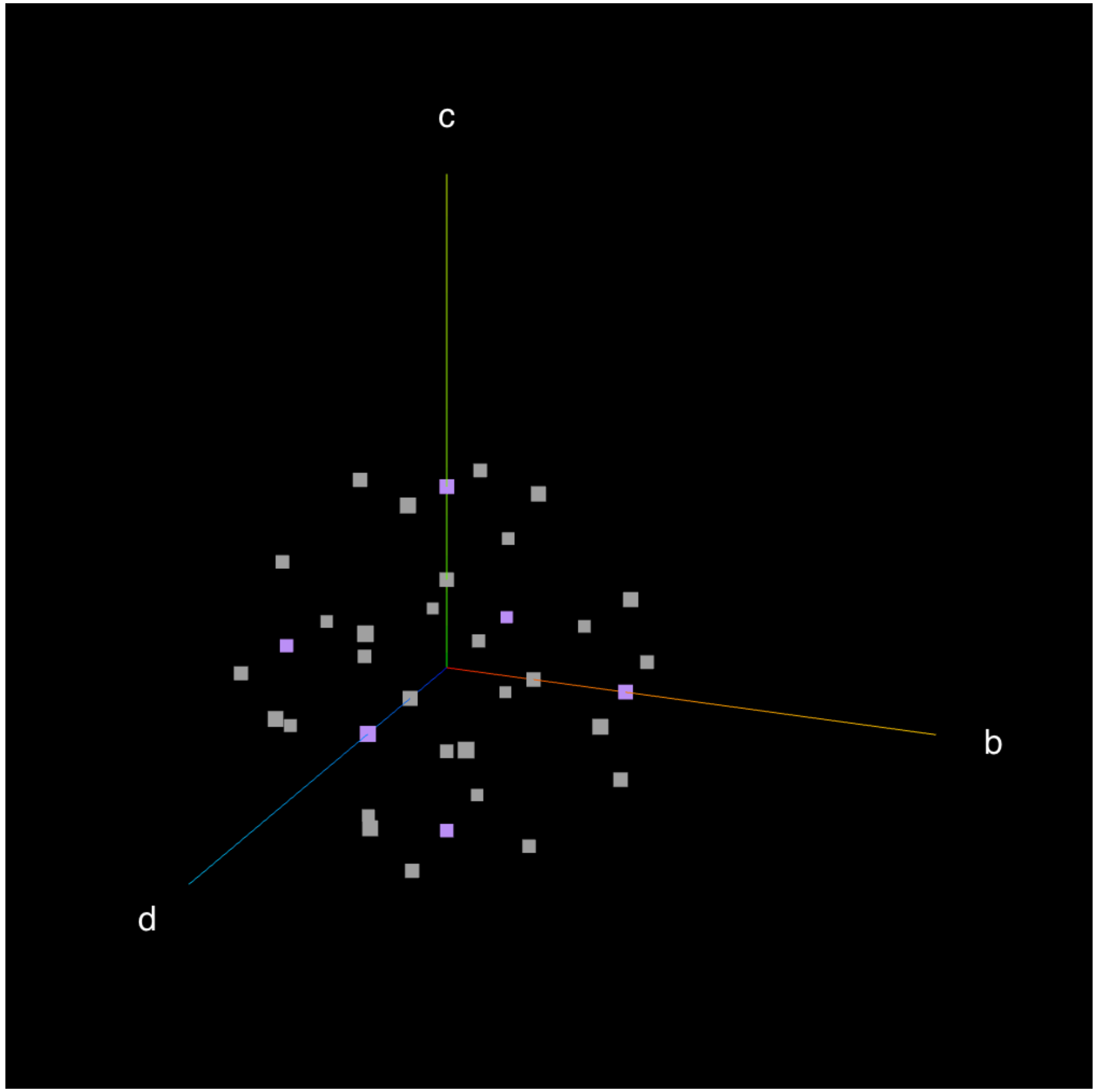
Theorem (Vaserstein): If $\begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \leq \Gamma \leq \mathrm{SL}_2(A)$, then $\Gamma \sim \mathrm{SL}_2(A)$ for $\mathbb{Z} \lneq A \leq \overline{\mathbb{Q}}$

Back to the globe game:

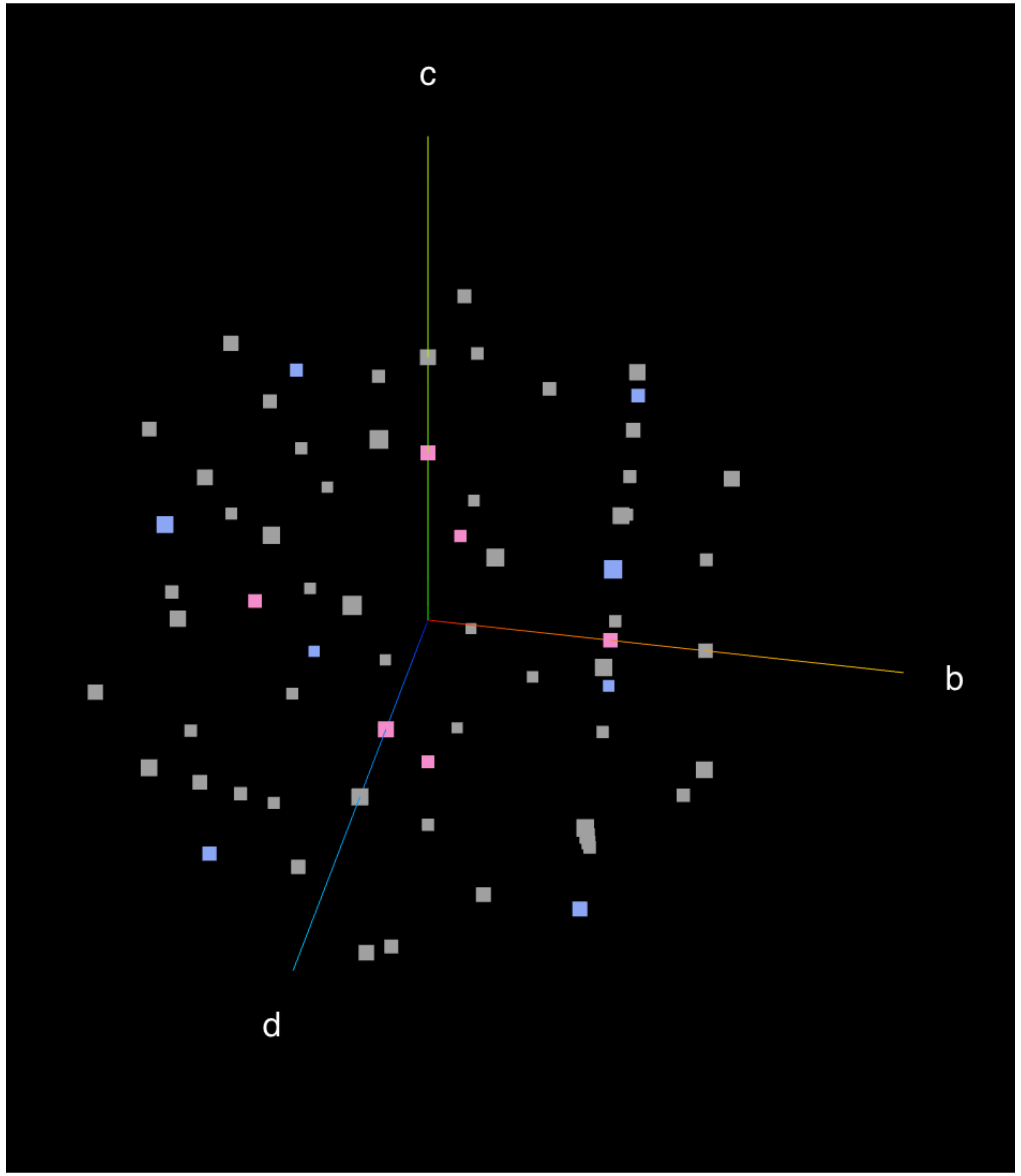
Recall Santa Cruz's precise coordinates are $\frac{1}{105625}\begin{pmatrix}-44568\\-71676\\63505\end{pmatrix}$,

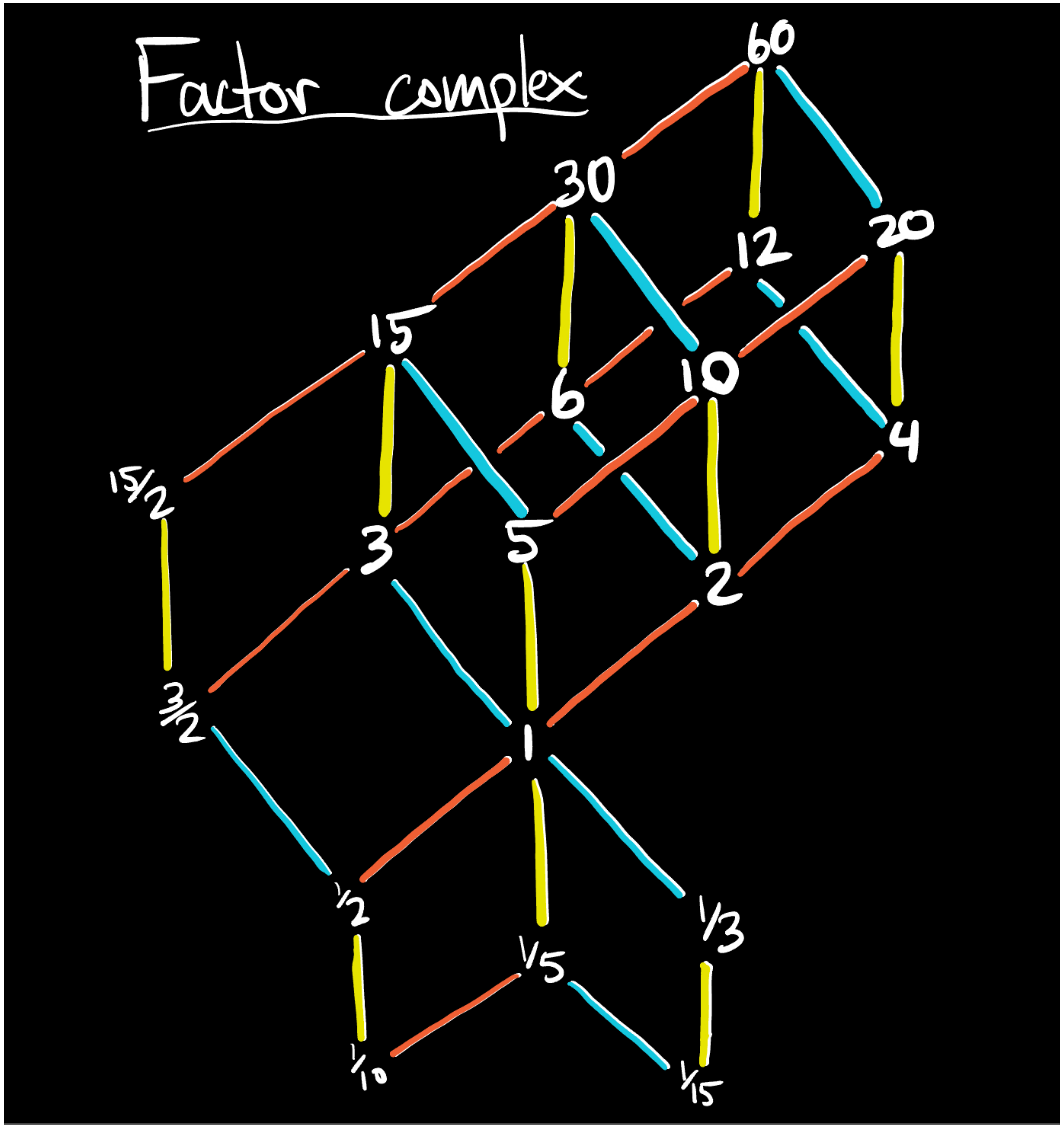
and Nashville is located at $\frac{1}{105625}\begin{pmatrix}4644\\-85175\\62292\end{pmatrix}$

Quaternions of norm 5

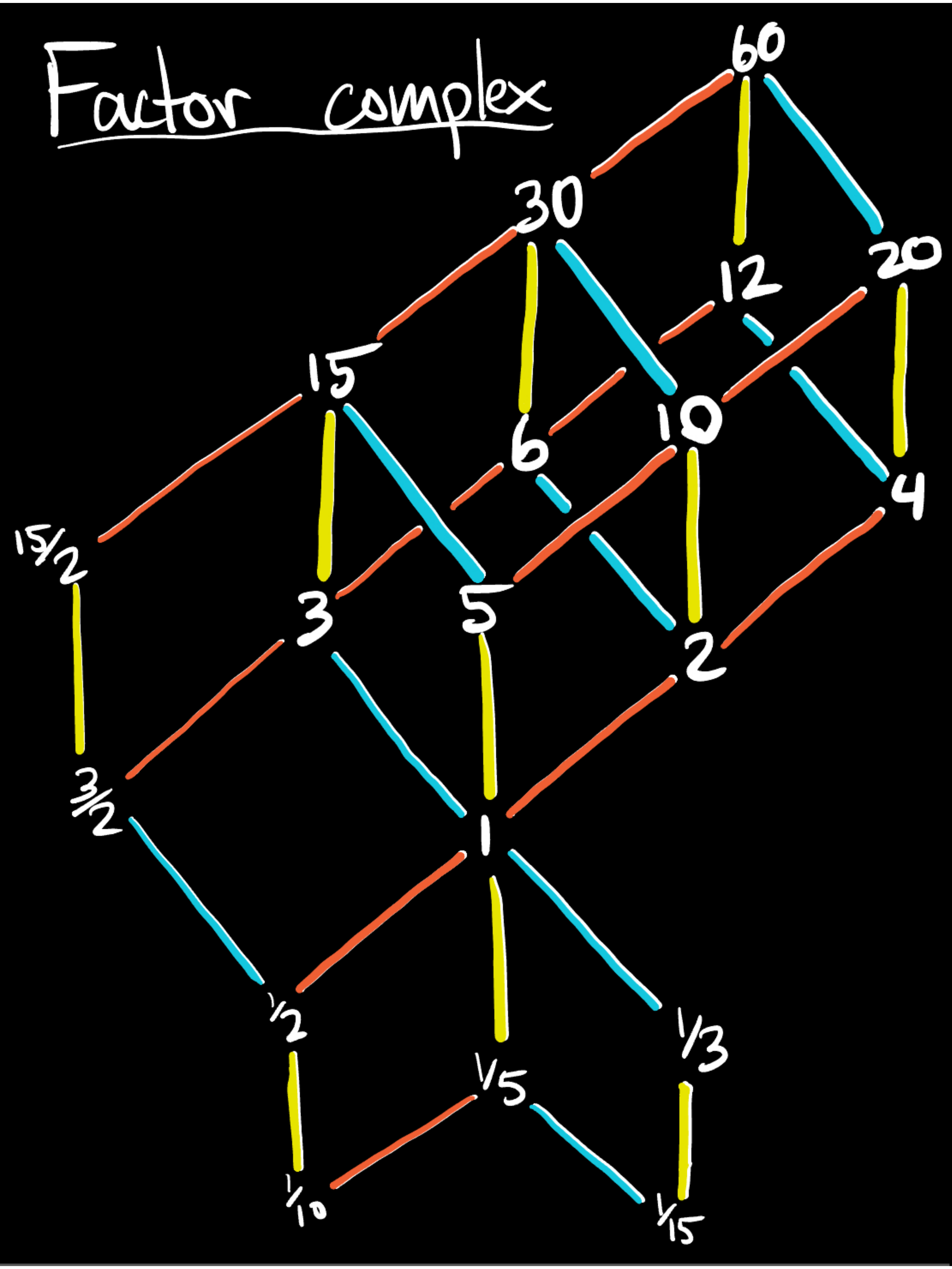


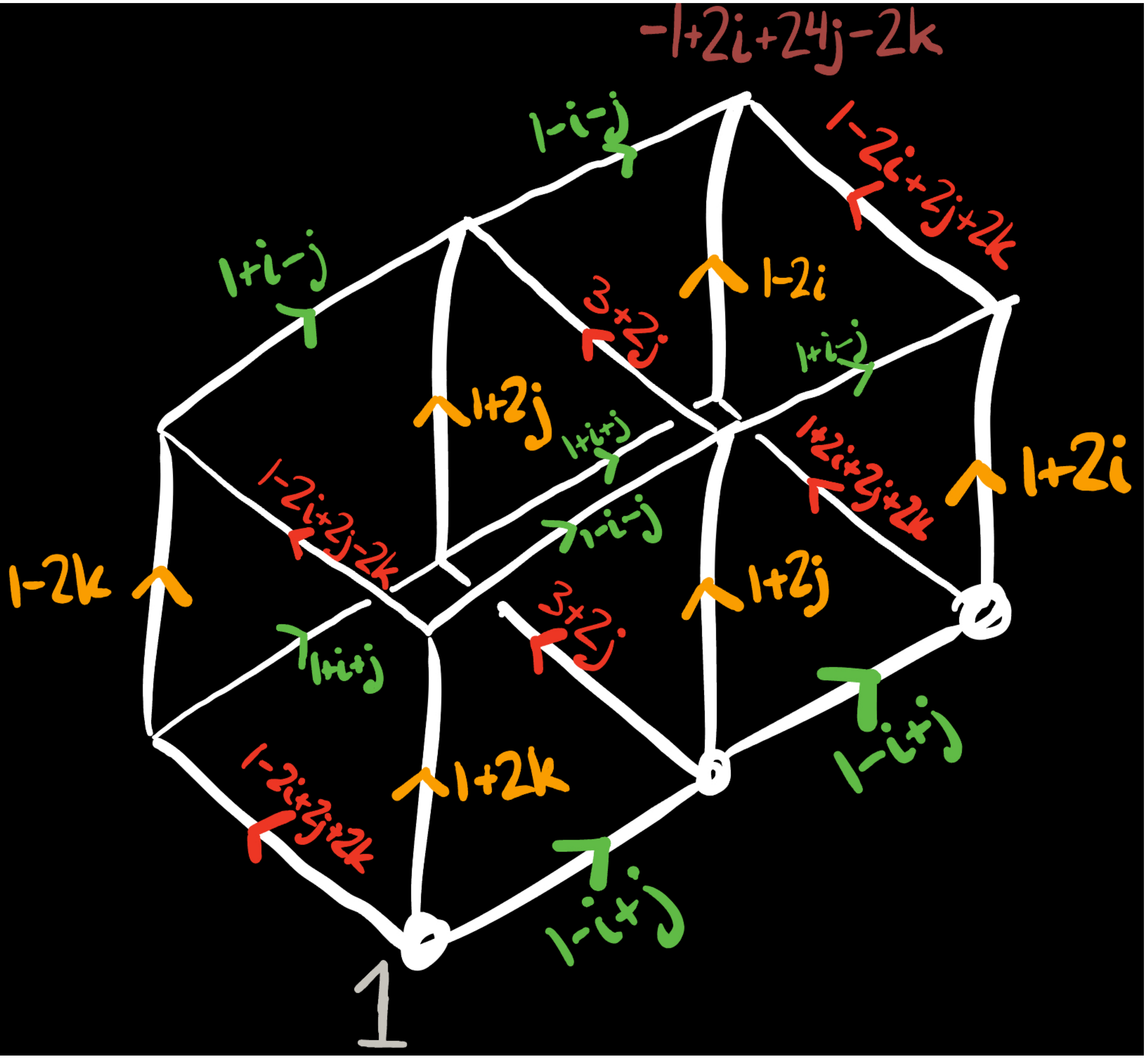
Quaternions of norm 13




Factor complex
60
30
12
20
15
6
10
4
15/2
3
5
2
3/2
1
1/2
1/5
1/3
1/10
1/15

Factor complex



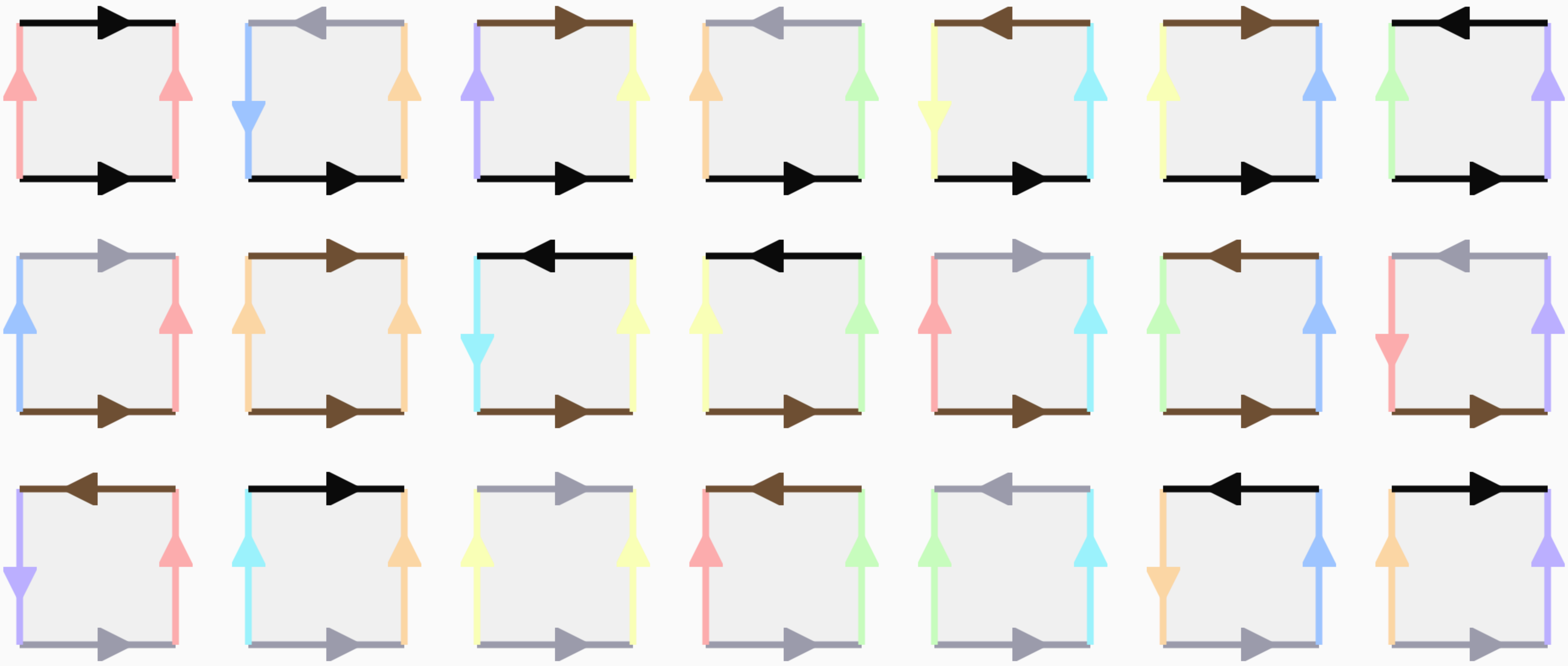


Generators

1+2i 1+2j 1+2k

3+2i 3+2j 3+2k 1+2i+2j+2k 1+2i+2j-2k 1+2i-2j+2k 1-2i+2j+2k

Relations

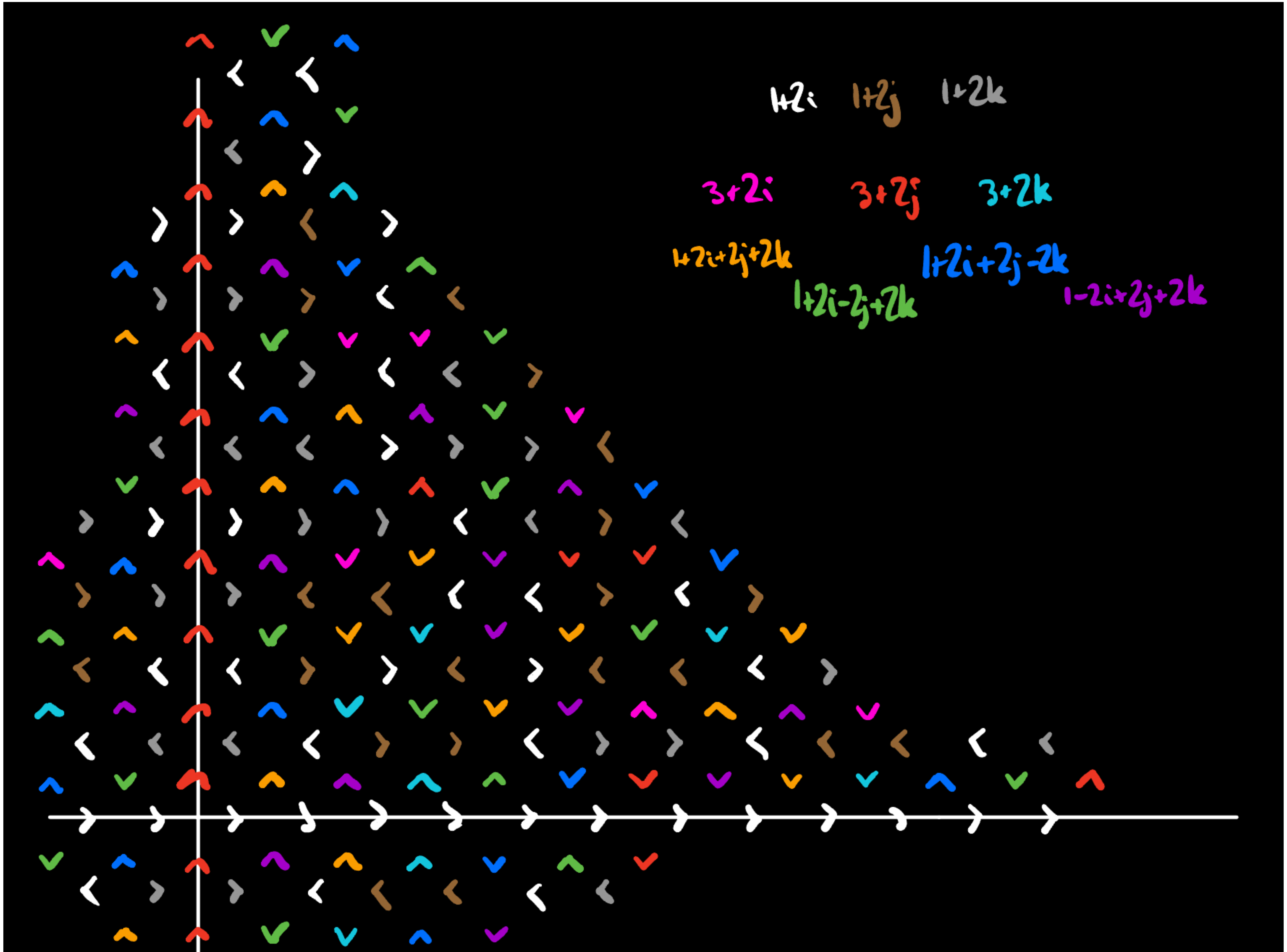


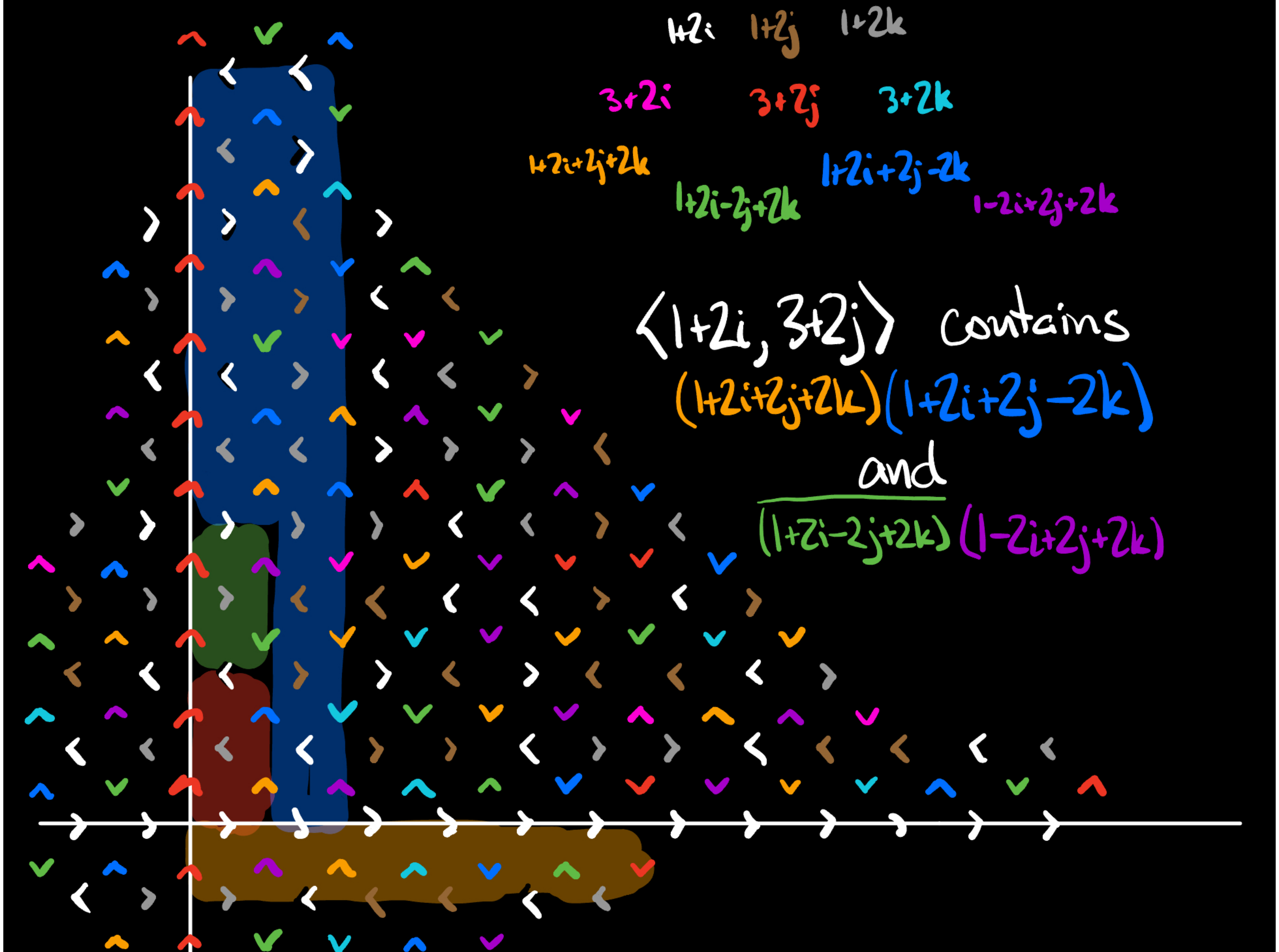
$$(j+k)(1+2k)(1+2k)(1+2i)(1-2j)(1-2i-2j-2k)(1-2i+2j+2k)\ldots$$

$$(3-2i)(1+2i+2j+2k)(1-2k)(1-2j)(1+2i)(1-2k)$$

is a shortest path in the cube complex which maps Santa Cruz to Nashville!

If we can write each element of this product as a word in the two rotation generators, we have a solution to the game.


1+2i
1+2j
1+2k
3+2i
3+2j
3+2k
1+2i+2j+2k
1+2i-2j+2k
1+2i+2j-2k
1-2i+2j+2k



1+2i 1+2j 1+2k
3+2i 3+2j 3+2k
1+2i+2j+2k 1+2i-2j+2k 1+2i+2j-2k 1-2i+2j+2k
⟨1+2i, 3+2j⟩ contains
(1+2i+2j+2k)(1+2i+2j−2k)
and
(1+2i−2j+2k)(1−2i+2j+2k)

The group $\langle 1+2i, 3+2j \rangle$ surjects every congruence quotient of $\mathrm{SO}_3(\mathbb{Z}[1/65])$. The preceding theorem then implies that the group is $\mathrm{SO}_3(\mathbb{Z}[1/65])$!

However, we have not yet succeeded in writing the set of standard generators as words in a and b.

Left/Right: rotate by 53.1301°.
Up/Down: rotate by 67.3801°.

Distance to Target: 1932.2 miles

Goal: Navigate the globe using the arrow keys. Try to move the character from the green beacon to the orange beacon.

Move Sequence

```
(no moves yet)
```

Matrix from word

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

Saved Rotations

Save current as g

Click to apply. Hold `Shift` to apply the inverse.

Controls:
- Arrow Keys: Rotate globe
- Mouse: Drag to orbit view
- Scroll: Zoom in/out

Thank you!