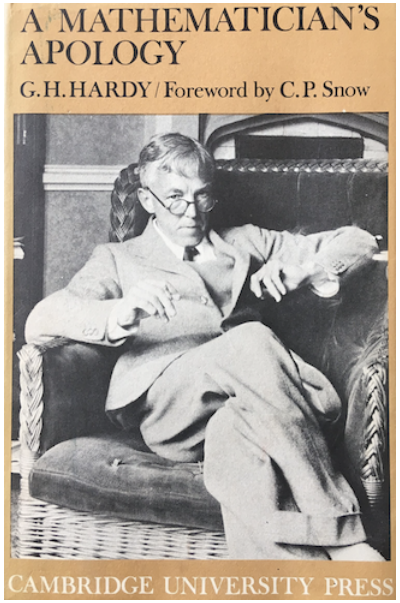
Chapter 1: Groups, intuitively

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Visual Algebra

The science of patterns



G.H. Hardy (1877–1947) famously said that "*Mathematics is the Science of Patterns*."

He was also the PhD advisor to the brilliant Srinivasa Ramanujan (1887–1920), the central character in the 2015 film *The Man Who Knew Infinity*.

In his 1940 book *A Mathematician's Apology*, Hardy writes:

> *"A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas."*

Another theme is that the inherent beauty of mathematics is not unlike elegance found in other forms of art.

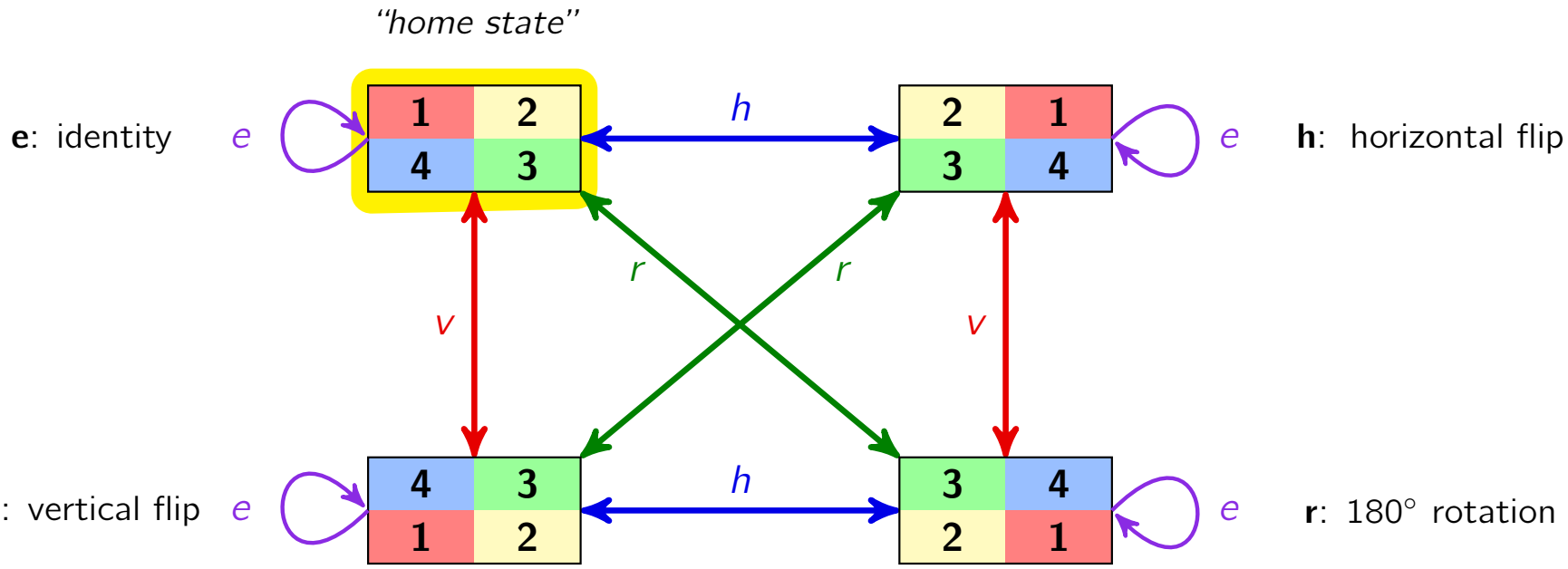
> *"The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way."*

Very few mathematical fields embody visual patterns as well as group theory.

We'll motivate the idea of a group by starting with the symmetries of a rectangle.

Our first group

The four symmetries of a rectangle can be visualalized using a **Cayley graph**, named after British mathematician Arthur Cayley (1821–1895).



The set **Rect** $= \{e, h, v, r\}$ of four symmetries is our first example of a **group**.

Observations?

Groups, informally

A group is a set of actions, satisfying a few mild properties.

Basic properties

- **Closure**: Composing actions in any order is another action.
- **Identity**: There is an identity action e, satisfying

$$ae = a = ea$$

  for all actions a. [*Often we use* 1 *instead of* e.]
- **Inverses**: Every action a in has an inverse action b, satisfying

$$ab = e = ba.$$

We call the operation of composing actions multiplication, and write it from left-to-right.

Every group has a generating set, and we use angle brackets to denote this.

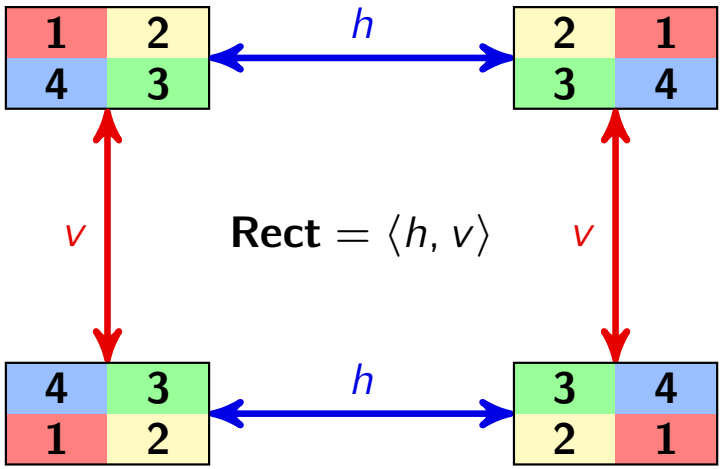
We usually prefer to find a minimal generating set. For example,

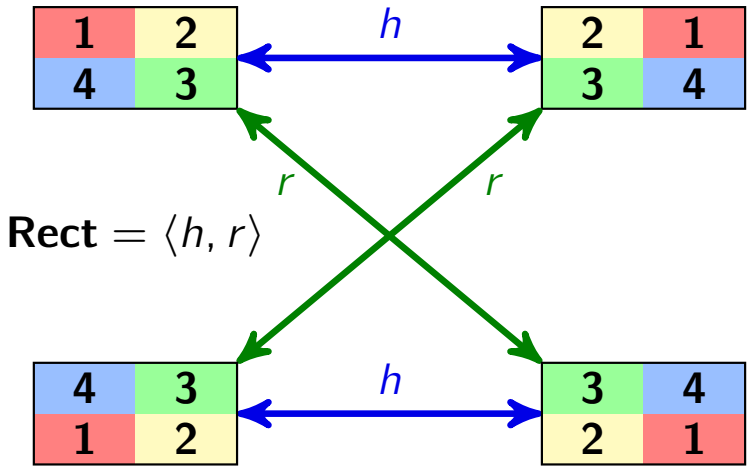
$$\textbf{Rect} = \langle v, h\rangle = \langle v, r\rangle = \langle h, r\rangle = \langle v, h, r\rangle = \langle v, h, e\rangle = \cdots$$

There still something missing from the above definition of a group. (Stay tuned!)

Minimal generating sets

Different minimal generating sets might lead to different Cayley graphs:





Remarks

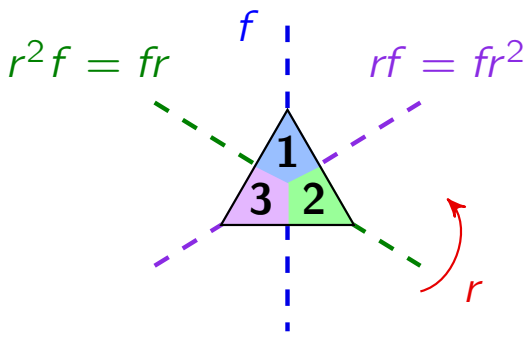
The group **Rect** has some properties that are not always true for other groups:

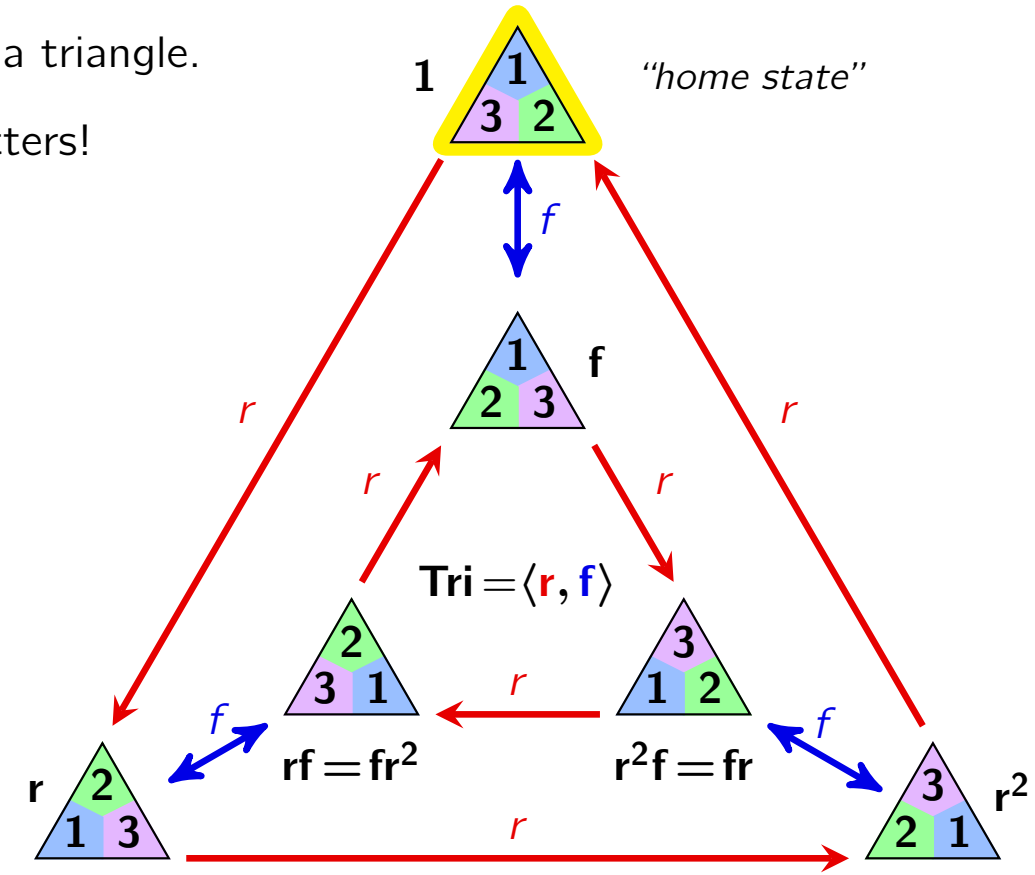
- it is **abelian**: $ab = ba$ for all $a, b \in$ **Rect**
- every element is its own inverse: $a^{-1} = a$ for all $a \in$ **Rect**
- the Cayley graphs for any two minimal generating sets have the same structure
- all minimal generating sets have the same size.

Symmetries of a triangle

Consider the group of symmetries of a triangle.

This group is **nonabelian** – order matters!





Equivalences of actions like the following are called relations:

$$r^3 = 1, \qquad f^2 = 1, \qquad rf = fr^2, \qquad fr = r^2f.$$

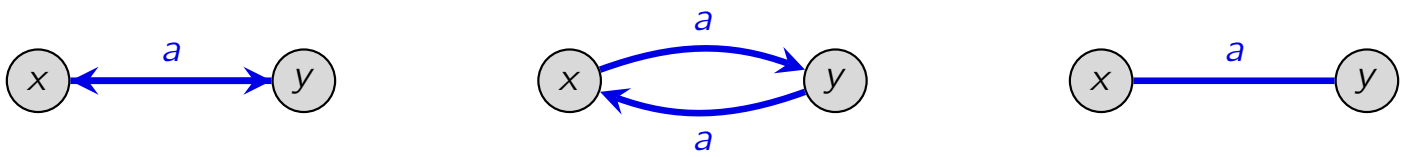
The Cayley graph makes it easy to find the inverse of each action:

$$1^{-1} = 1, \qquad r^{-1} = r^2, \qquad (r^2)^{-1} = r, \qquad f^{-1} = f, \qquad (rf)^{-1} = rf, \qquad (r^2f)^{-1} = r^2f.$$

Cayley graph structure

Any action with $a^2 = 1$ is its own inverse: $a^{-1} = a$.

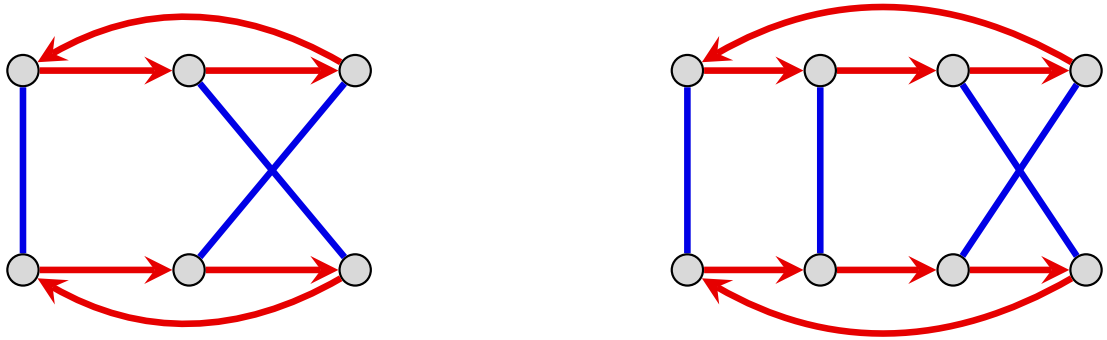
When this happens, we will use undirected arrows instead of bi-directed or double arrows:



Four of the six actions in **Tri** $= \langle r, f \rangle$ are their own inverse.

Cayley graphs must have a certain regularity: if $rf = fr^2$ holds from one node, it must hold from *every* node.

Do either of the following graphs have this regularity property?



A different generating set for the triangle symmetry group

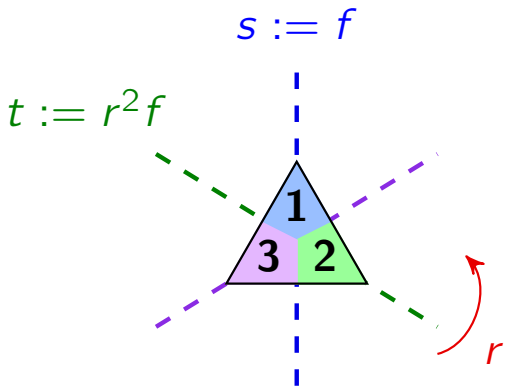
Recall the triangle symmetry group

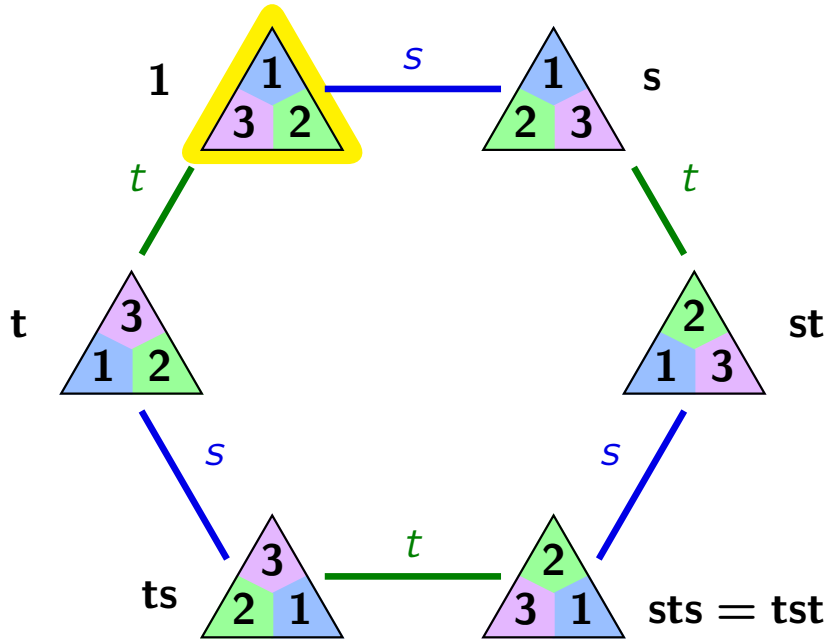
$$\mathbf{Tri} = \{ \underbrace{1,\ r,\ r^2}_{\text{rotations}},\ \underbrace{f,\ rf,\ r^2 f}_{\text{reflections}} \}.$$

Notice that the composition of two reflections is a 120° rotation:

$$(rf) \cdot f = rf^2 = r \cdot 1 = r, \qquad f \cdot rf = f \cdot fr^2 = 1 \cdot r^2 = r^2.$$

Let's see a Cayley graph corresponding to $\mathbf{Tri} = \langle s, t \rangle$, where $s := f$ and $t := r^2 f = fr$.





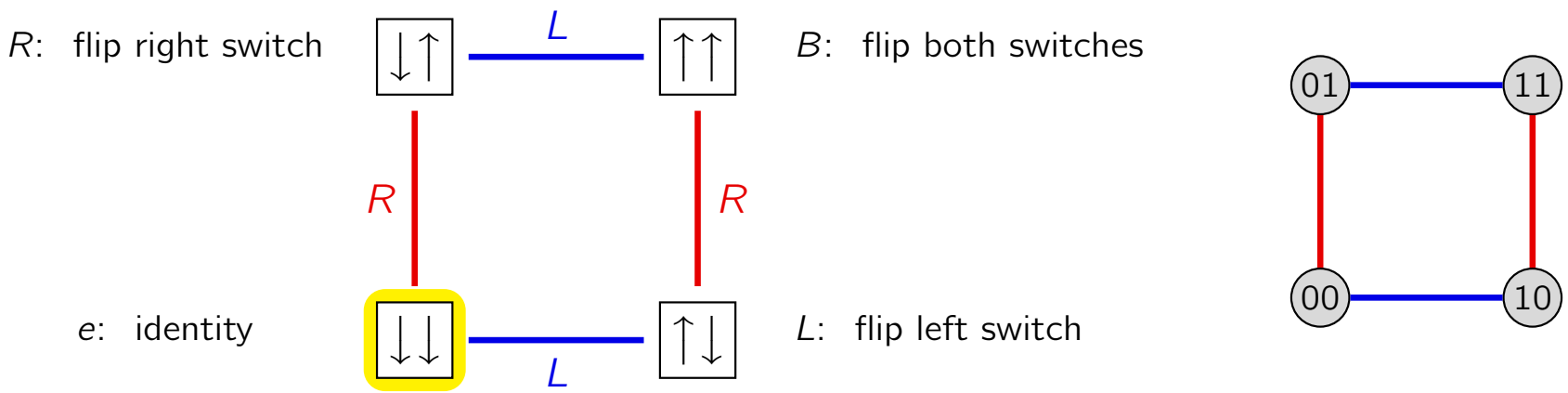
Groups arising from non-symmetry actions

Consider two light switches in the "down" position. Call this our "home state".

Let $\mathbf{Light}_2 = \langle L, R \rangle$ be the group, where

- L: flip left switch
- R: flip right switch

Here is a Cayley graph:



Remark

The Cayley graphs for $\mathbf{Rect} = \{e, v, h, r\}$ and $\mathbf{Light}_2 = \{e, L, R, B\}$ have the same structure. We say they are isomorphic, and write

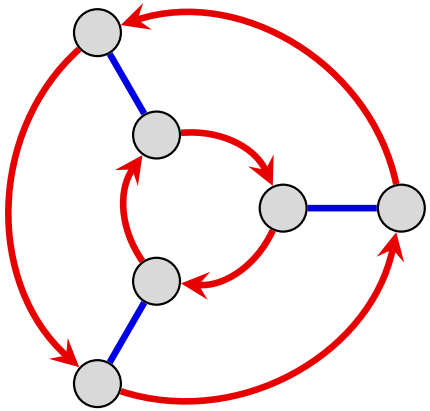
$$\mathbf{Rect} \cong \mathbf{Light}_2 .$$

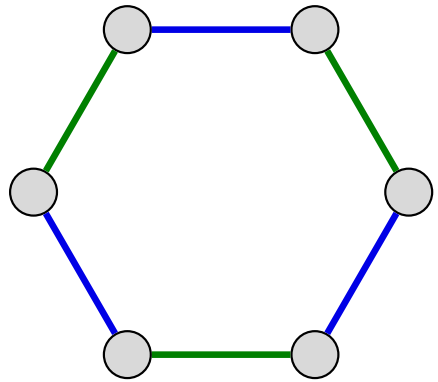
Isomorphic groups

The formal definition of two groups being isomorphic is technical, and involves a structure preserving bijection between them.

If two groups have generating sets that define Cayley graphs of the same structure, they are isomorphic, and we have a "*Yes Certificate*".

If the Cayley graphs are different, then the groups are not necessarily non-isomorphic, as we saw with **Tri** $= \langle r, f \rangle = \langle s, t \rangle$.





In other words, a "*No Certificate*" is harder to verify.

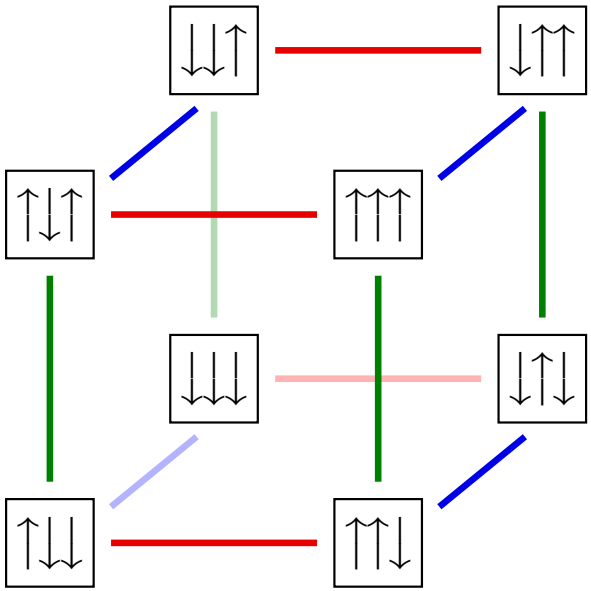
Remark

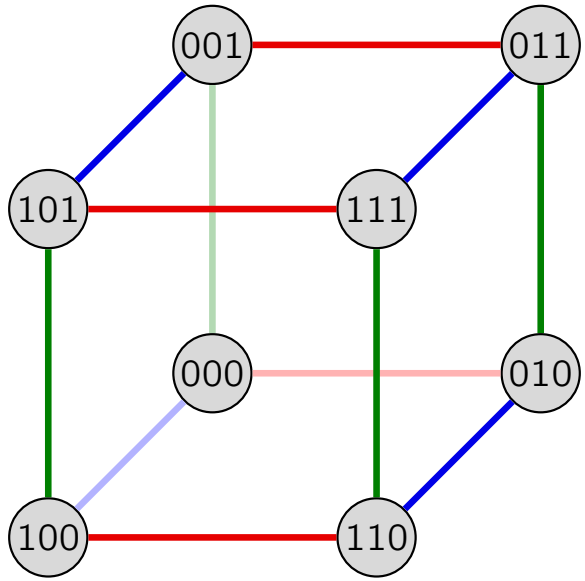
To prove two groups are non-isomorphic, find a property that one has but the other doesn't.

The three light switch group

The "2 *light switch group*" generalizes to the "3 *light switch group*" in the obvious manner:

$$\textbf{Light}_3 := \langle L, M, R \rangle.$$





Properties of $\textbf{Light}_3$

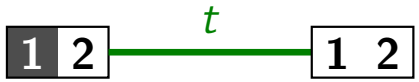
- this group is abelian: $ab = ba$, for all $a, b \in \textbf{Light}_3$
- every action is its own inverse: $a^2 = e$, or $a^{-1} = a$, for all $a \in \textbf{Light}_3$ (*verify!*)
- any minimal generating set has size 3 (*not immediately obvious*).

Another group of size 8

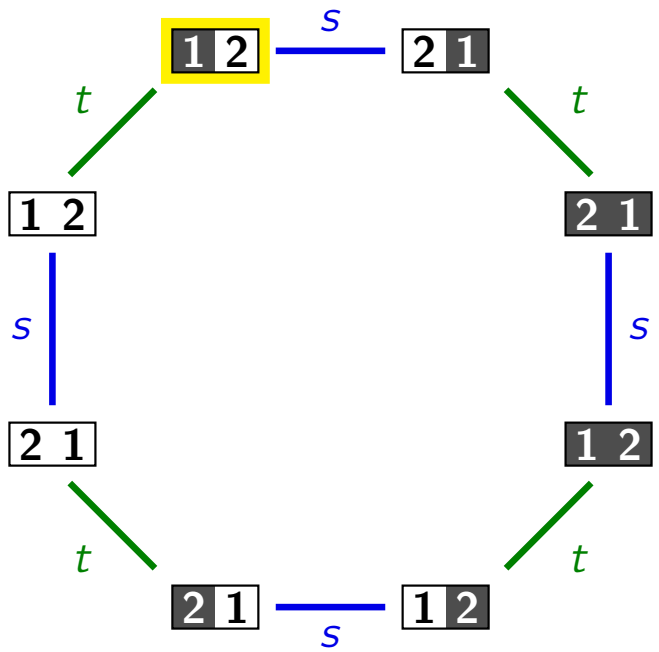
Call the following rectangle configuration our *home state*: 

Suppose we are allowed the following operations, or "actions":

- s: swap the two squares
- t: toggle the color of the first square.



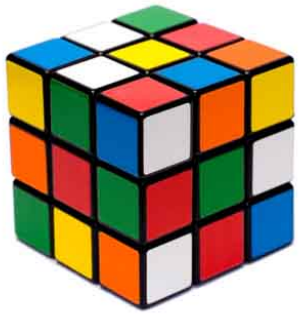
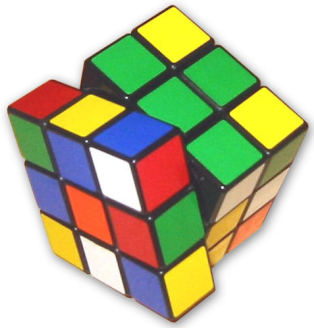
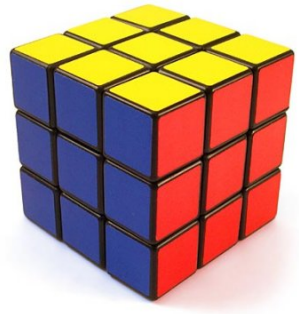
Here is a Cayley graph of this group that we'll call $\mathbf{Coin}_2 = \langle s, t \rangle$:



Question: *Are the groups* $\mathbf{Coin}_2$ *and* $\mathbf{Light}_3$ *isomorphic?*

The Rubik's cube group

One of the most famous groups is the set of actions on the Rubik's Cube.

Fact

There are 43,252,003,274,489,856,000 distinct configurations of the Rubik's cube.

This toy was invented in 1974 by architect Ernő Rubik (born 1944) of Budapest, Hungary.

His Wikipedia page used to say:

> He is known to be an introvert and hardly accessible person, hard to contact or get for autographs. He typically does not attend speedcubing events. However, he attended the 2007 World Championship in Budapest.[2][3]

The Rubik's cube group

Not impossible . . . just almost impossible.

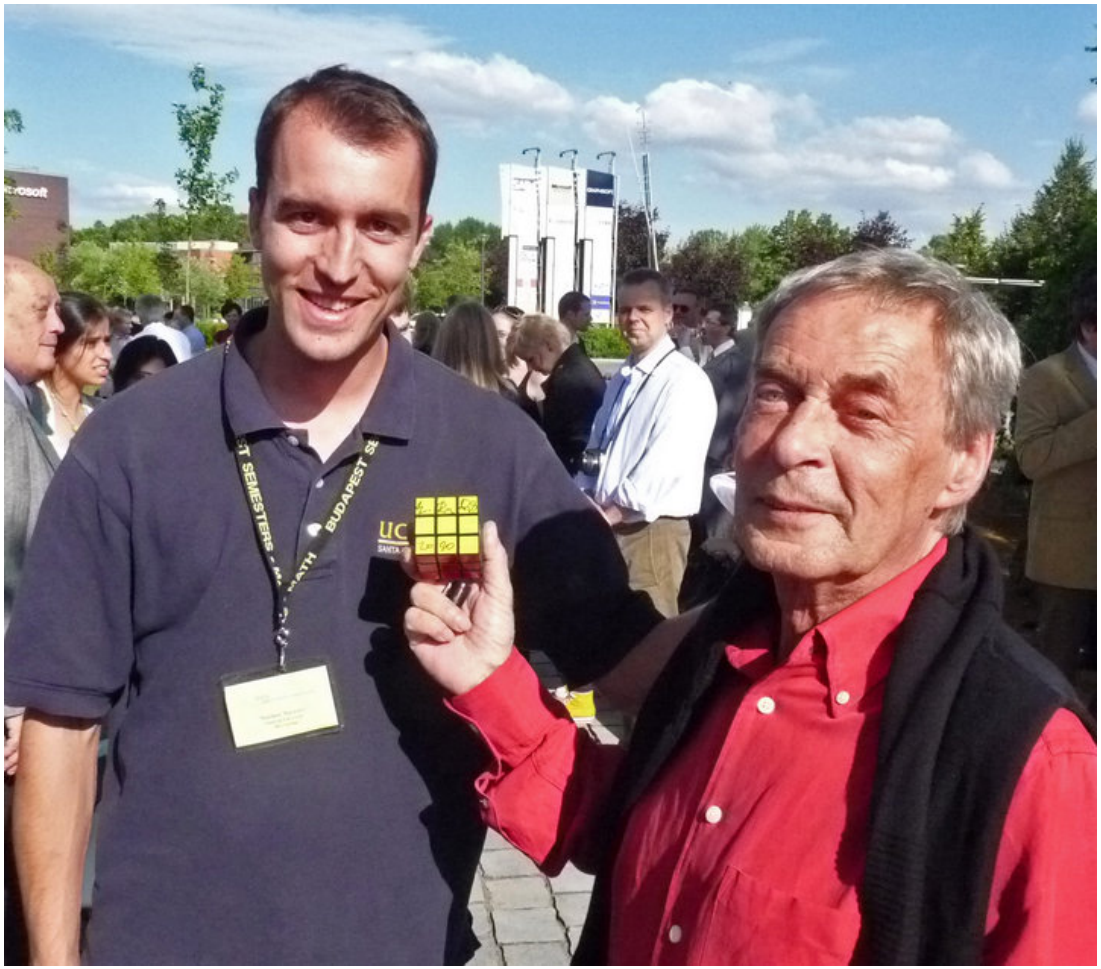


Figure: June 2010, in Budapest, Hungary

The Rubik's Cube group

The configurations of the Rubik's cube are different than the actions, but they are in bijective correspondence.

The Rubik's cube group is generated by 6 actions:

$$\textbf{Rubik} := \langle F,\ B,\ R,\ L,\ U,\ T \rangle,$$

where

- F: front face, 90° clockwise turn.
- B: back face, 90° clockwise turn.
- R: right face, 90° clockwise turn.
- L: left face, 90° clockwise turn.
- U: upper face, 90° clockwise turn.
- T: top face, 90° clockwise turn.

In other words, these six actions generate all $\left|\textbf{Rubik}\right| = 43{,}252{,}003{,}274{,}489{,}856{,}000$ actions of the Rubik's cube group.

Theorem (2010)

Every configuration of the Rubik's cube group is at most 20 "moves" from the solved state. Moreover, there are configurations that are exactly 20 moves away.

The Rubik's Cube group

Though the Rubik's cube group is generated by 6 actions,

$$\textbf{Rubik} := \langle F,\ B,\ R,\ L,\ U,\ T \rangle,$$

most solution guides also use:

- F', B', R', L', U', T' for 90° counterclockwise turns, and
- $F2, B2, R2, L2, U2, T2$ for 180° turns.

The theorem about "*every configuration is at most* 20 *moves away*" considers this definition for a "*move*."

The following is a standard definition from graph (or network) theory.

Definition

The diameter of a graph is the longest shortest path between any two nodes.

Theorem (2010)

The diameter of the Cayley graph of the Rubik's cube group, with generating set

$$\textbf{Rubik} = \langle F, B, R, L, U, D, F', B', R', L', U', D', F2, B2, R2, L2, U2, D2 \rangle$$

is 20.

The Rubik's Cube group

In 2014, Tomas Rokicki and Morley Davidson, with the Ohio Supercomputing Center, solved the Rubik's cube in the "*quarter-turn metric*".

Theorem (2014)

The diameter of the Cayley graph of the Rubik's cube group, with generating set

$$\textbf{Rubik} = \langle F, B, R, L, U, D, F', B', R', L', U', D' \rangle$$

is 26.

In the "*half-turn metric*," there are hundreds of millions of nodes a maximal distance (exactly 20) from the solved state.

In the "*quarter-turn metric*," we only know of three at a maximal distance (exactly 26).

It is conjectured that there are

- $\approx$ 36 nodes at a distance of 25
- $\approx$ 150,000 nodes at a distance of 24
- $\approx$ 24 quadrillion (2.4×10^{16}) nodes at a distance of 23.

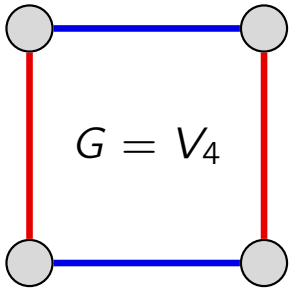
When we study permutation groups, we'll learn why the quarter-turn metric is more natural than the half-turn metric.

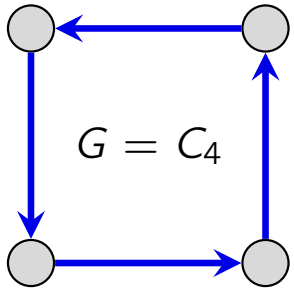
Unlabeled Cayley graphs

Previously, we've labeled the nodes of Cayley graphs with configurations.

If we want to focus on a graph's structure, we can leave the nodes unlabeled.

For example, consider the following two groups of size 4:





The abstract group isomorphic to **Rect** is the Klein 4-group, denoted V_4, named after German mathematician Felix Klein (1849–1925).

Questions

- Are the two groups whose Cayley graphs shown above isomorphic?
- Can you think of an object whose symmetry group has the group on the right?

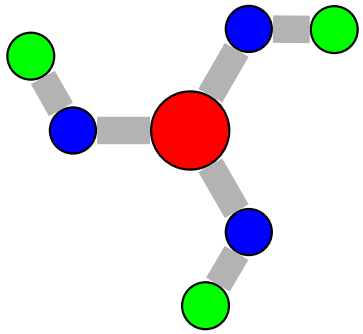
Cyclic groups (preview)

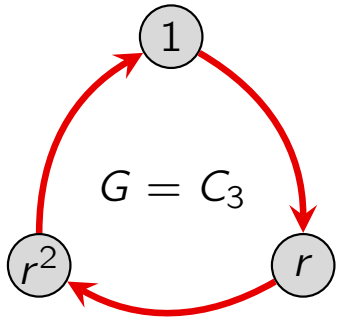
Groups that can be generated by a single action are called cyclic.

These describe shapes that have only rotational symmetry.

The shape of a molecule of boric acid, $B(OH)_3$, is shown below. It should be clear that there are three symmetries:

- the identity action, 1
- 120° counterclockwise rotation, r
- 240° counterclockwise rotation, r^2.





The boric acid molecule is chiral because a mirror reflection is not a symmetry.

Inorganic chemists use groups theory to classify molecules by their symmetries.

The triangle symmetry group **Tri** $= \langle r, f \rangle$ contains $C_3 = \langle r \rangle$ as a subset. We say that C_3 is a subgroup of **Tri**.

Labeling Cayley graphs with actions

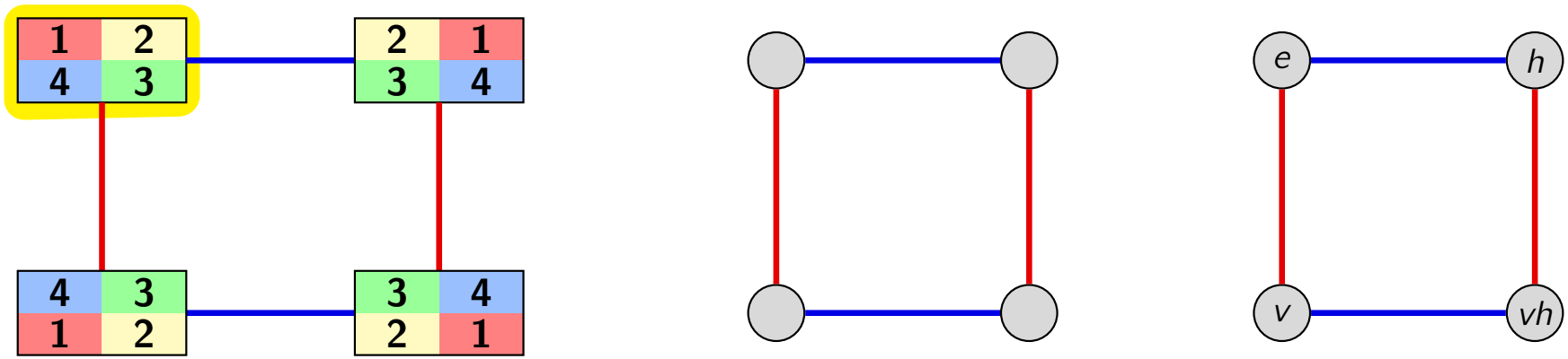
When drawing Cayley graphs, we have done one of two things with the nodes:

1. Label nodes with configurations of an object
2. Leaving nodes unlabeled

There is a 3rd choice, since every path represents an action in the group.

3. Label the nodes with actions.

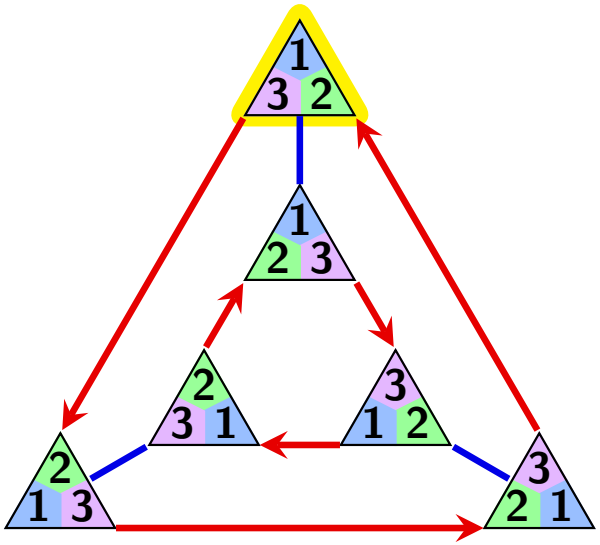
Here is one way to do this for the Klein 4-group, $G = V_4$:

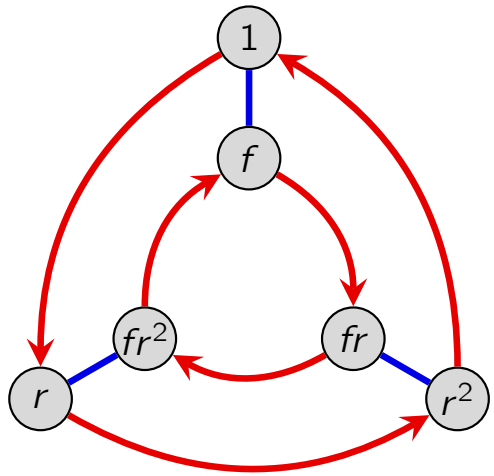


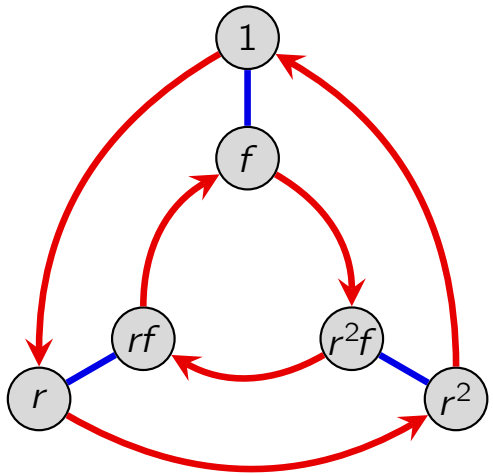
By the "regularity property" of Cayley graphs, it does not matter where we start, or what path we take when labeling.

Labeling Cayley graphs with actions

Here are two canonical ways to label the nodes of the Cayley graph of $\mathbf{Tri} = \langle r, f \rangle$.







Technically, these are right Cayley graphs because we are reading from left-to-right.

In other words, traversing around the graph corresponds to right multiplication.

Remark

Every path corresponds to an action $a \in G$. To compute a path for $ab \in G$:

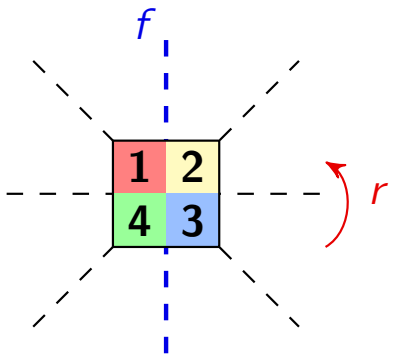
- start at node a (or equivalently, start at the identity node and follow any path for a).
- follow any path corresponding to b.

Another group of size 8

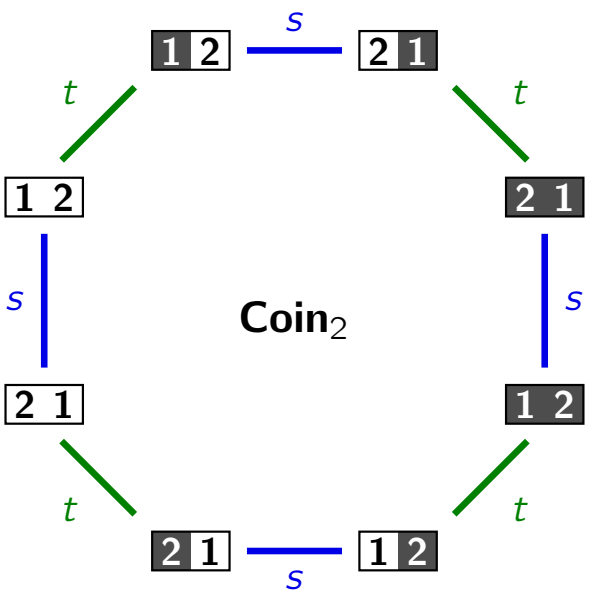
The eight symmetries of a square form a group generated by:

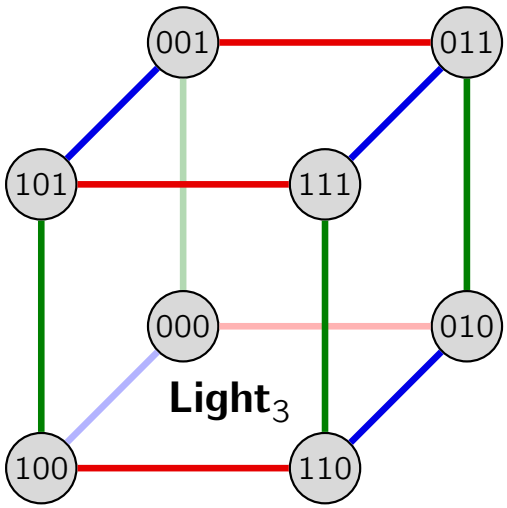
- a 90° counterclockwise rotation r,
- a horizontal flip f.

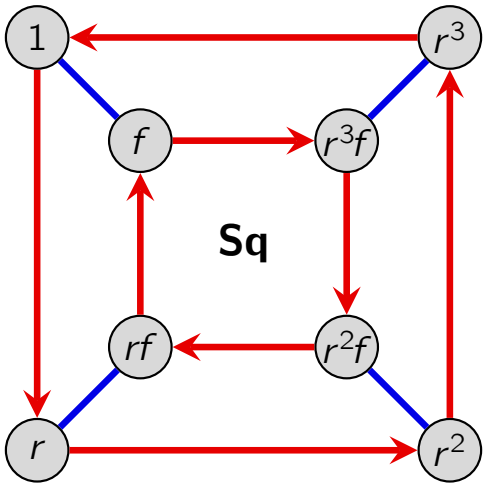
We'll call this group $\mathbf{Sq} = \langle r, f \rangle$.



Question: *Do any of these groups have the same structure? (Are they "isomorphic"?)*







Can you find a property that one group (not graph!) has that the others do not?

Group presentations

Thus far, we've described a group by its generators.

$G = \langle r, f \rangle$ means "*G is generated by r and f*."

However, this doesn't tell us *how* they generate.

Definition

A group presentation for G is a description of the group as

$$G = \left\langle \text{generators} \;\middle|\; \text{relations} \right\rangle.$$

The vertical bar can be thought of as meaning "subject to".

Even for a fixed set of generators, a group presentation is not unique.

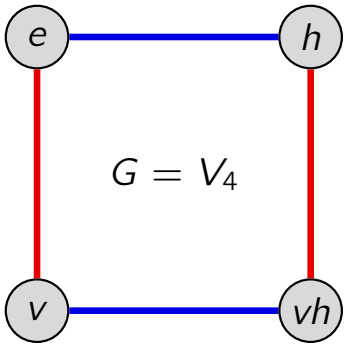
Key idea

A presentation is just an algebraic way to encode a Cayley graph.

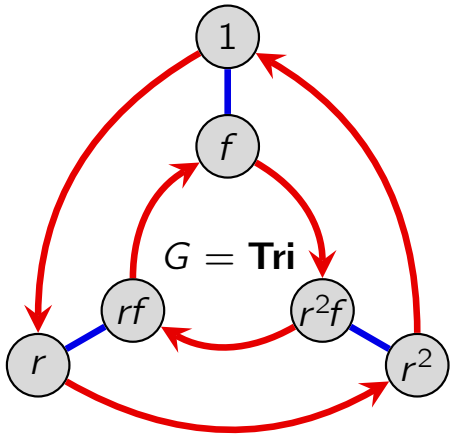
But, it doesn't necessarily tell us *which* Cayley graph!

Group presentations

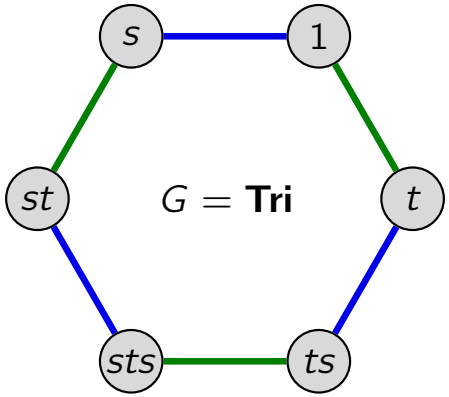
Here are some example of presentations:



$\langle v, h \mid v^2 = h^2 = e,\ vh = hv \rangle$



$\langle r, f \mid r^3 = f^2 = 1,\ rf = fr^2 \rangle$

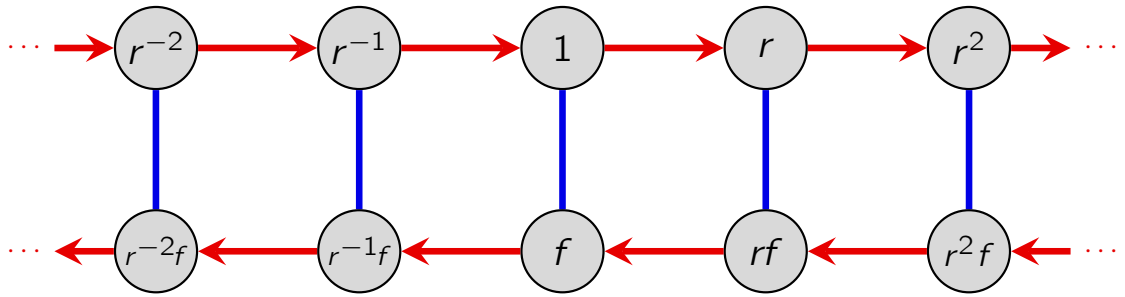


$\langle s, t \mid s^2 = t^2 = 1,\ sts = tst \rangle$

The relation $r^3 = 1$ is redundant in the second presentation:

$$rf = fr^2 \quad \Rightarrow \quad f(rf) = r^2 \quad \Rightarrow \quad (frf)^2 = r^4 \quad \Rightarrow \quad fr^2f = r^4 \quad \Rightarrow \quad (fr^2)f = r^4$$
$$\Rightarrow \quad (rf)f = r^4 \quad \Rightarrow \quad r = r^4 \quad \Rightarrow \quad 1 = r^3$$

But removing $r^3 = 1$ from $\mathbf{Tri} = \langle r, f \mid r^3 = f^2 = 1,\ rf = fr^{-1} \rangle$ yields an infinite group.



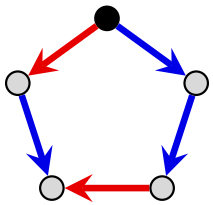
Group presentations

The word problem

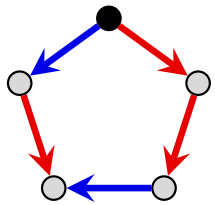
Given a presentation $G = \langle g_1, \ldots, g_n \mid r_1 = e, \ldots, r_m = e \rangle$, is $G = \{e\}$?

Exercise

Show that $G = \langle a, b \mid ab = b^2 a,\ ba = a^2 b \rangle$ is the trivial group.



$aba^{-1}b^{-2} = 1$ *and*



$bab^{-1}a^{-2} = 1$ $\Longrightarrow$

$G = \langle a, b, \mid a = b = 1 \rangle = \langle 1 \rangle$

An even harder problem is the isomorphism problem: Given G_1 and G_2, is $G_1 \cong G_2$?

Question

Given a group presentation that "looks like" a large group, *how can we be absolutely sure?*

Unsolvability of the word problem

Theorem

The word problem is unsolvable, even for finitely presented groups.

4-dimensional sphere problem

Given a 4-dimensional surface, determine whether it is homeomorphic to the 4-sphere.

Every surface S has a group $\pi_1(S)$ called the fundamental group of all "looped paths."

Four dimensions is big enough that for *any* G, we can build a surface for which $\pi_1(S) \cong G$.

Theorem

The 4-dimensional sphere problem is unsolvable.

Summary of the proof

Suppose there exists a solution, and let G be a group.

1. Build a surface S such that $\pi_1(S) \cong G$.
2. Determine whether S is a 4-sphere (all loops on a sphere are trivial).
3. This solves the word problem for G. (Contradiction)

Frieze groups

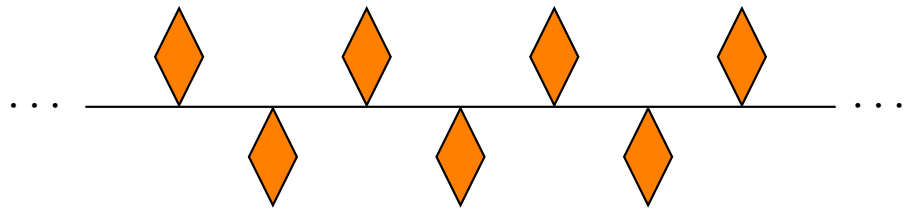
In architecture, a frieze is a long narrow section of a building, often decorated with art.

Figure: A frieze on the Admiralty, in Saint Petersburg.

They were common on ancient Greek, Roman, and Persian buildings.

Sometimes, but not always, such a pattern repeats.

In mathematics, a frieze is a 2-dimensional pattern that repeats in one direction, with a minimal nonzero translational symmetry.

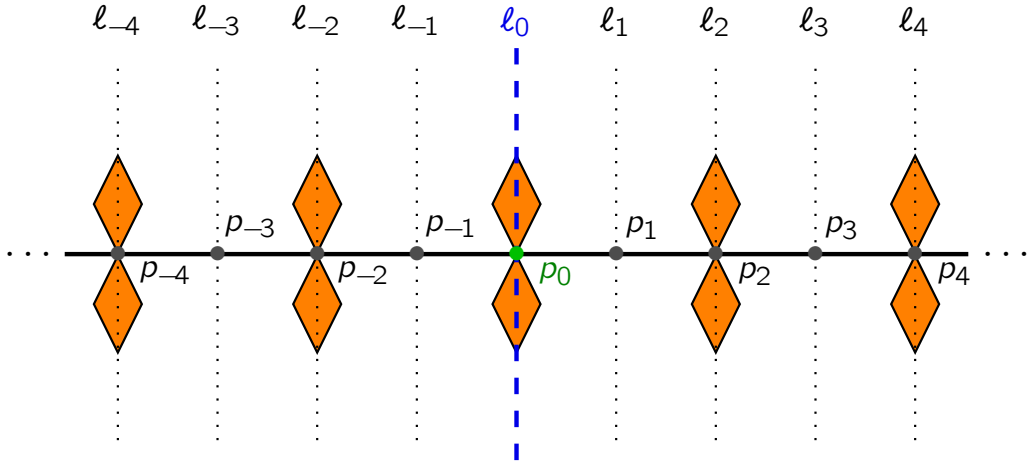


Definition

The symmetry group of a frieze is called a frieze group.

Goal. *Understand and classify the frieze groups.*

Frieze groups



Definition

Let v be the unique vertical reflection. Symmetries come in infinite families. Define

- t: minimal translation to the right
- h_i: horizontal reflection across ℓ_i
- $g_i := t^i v = v t^i$: glide-reflection
- r_i: 180° rotation around p_i

The symmetry group of this frieze consists of the following symmetries:

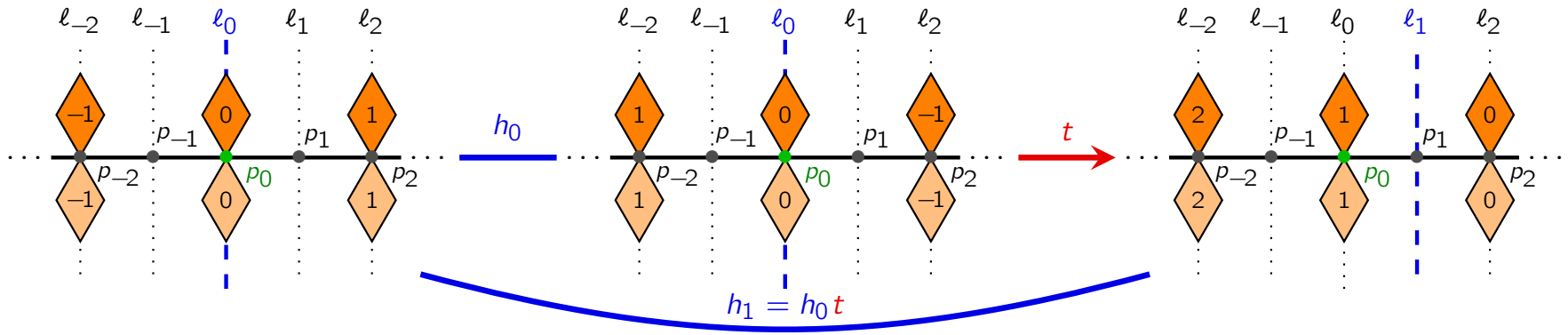
$$\mathbf{Frz}_1 := \{h_i \mid i \in \mathbb{Z}\} \cup \{r_i \mid i \in \mathbb{Z}\} \cup \{t^i \mid i \in \mathbb{Z}\} \cup \{g_i \mid i \in \mathbb{Z}\}.$$

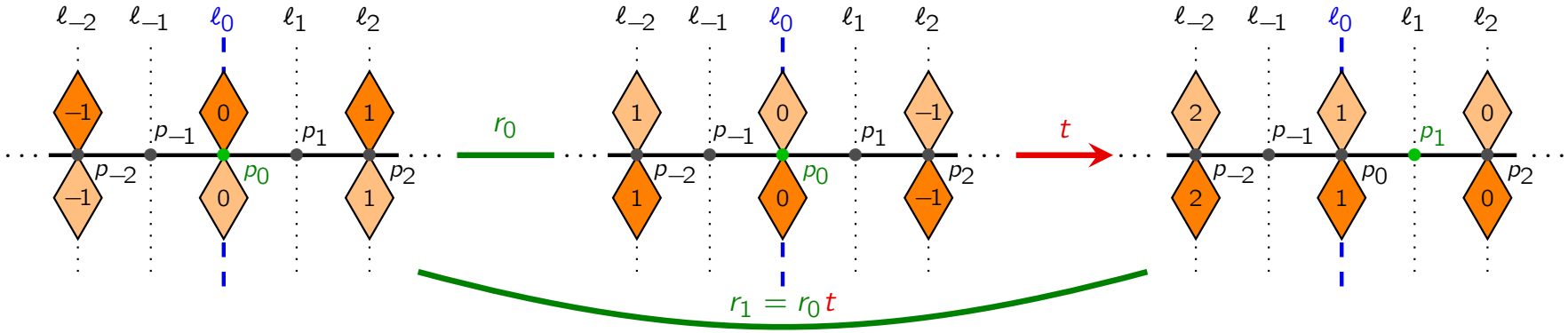
Note that $v = g_0$. Letting $h := h_0$, $r := r_0$, and $g := g_1$, this frieze group is generated by

$$\mathbf{Frz}_1 := \langle t, h, v \rangle = \langle t, h, r \rangle = \langle t, v, r \rangle = \langle g, h, v \rangle = \cdots$$

Frieze groups

Let's look at how the various reflections and rotations are related:

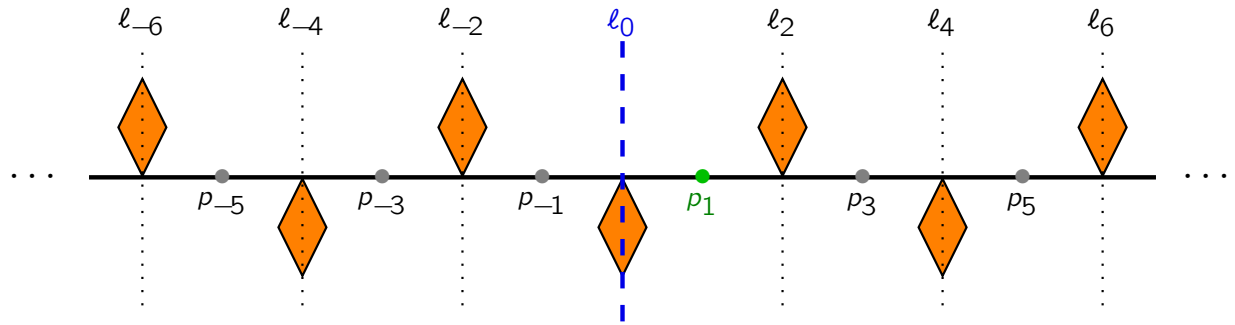




Similarly, it follows that $h_i\, t = h_{i+1}$ and $r_i\, t = r_{i+1}$ for any $i \in \mathbb{Z}$.

A "smaller" frieze group

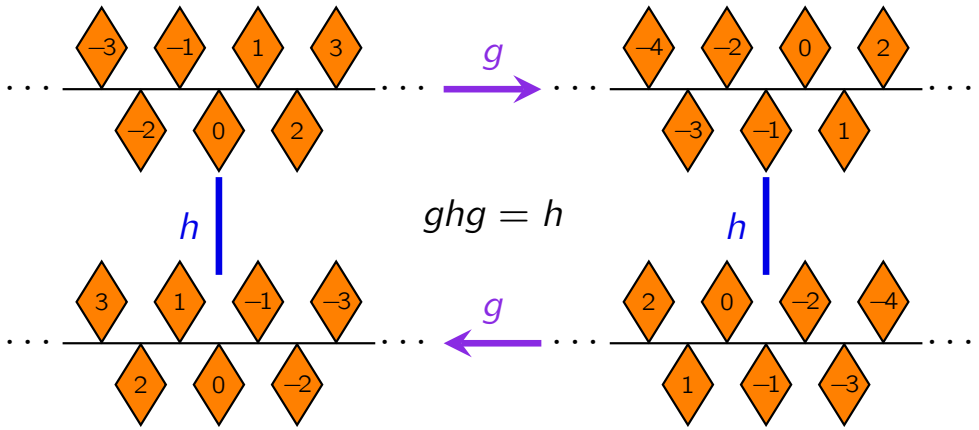
Let's eliminate the vertical symmetry from the previous frieze group.

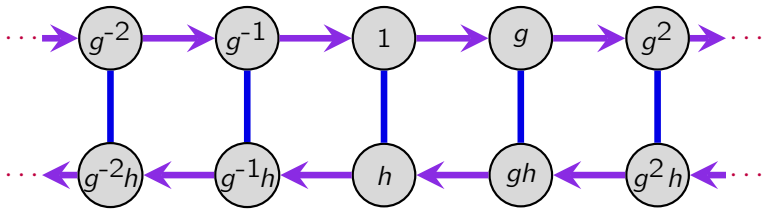


We lose half of the horizontal reflections and rotations in the process. The frieze group is

$$\mathbf{Frz}_2 := \{g^i \mid i \in \mathbb{Z}\} \cup \{h^{2j} \mid j \in \mathbb{Z}\} \cup \{r^{2k+1} \mid k \in \mathbb{Z}\} = \langle g, h \rangle = \langle g, r \rangle,$$

where $h = h_0$, $r = r_1$, $g = g_1 = tv$.

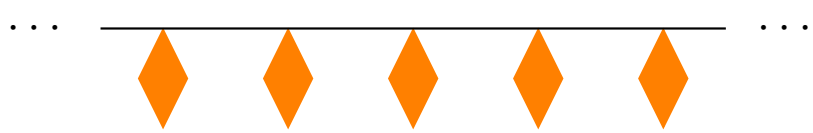


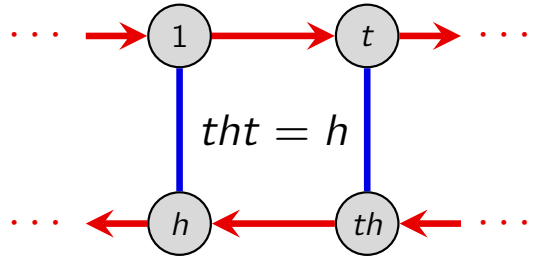


$$\mathbf{Frz}_2 = \langle g, h \mid h^2 = 1,\ ghg = h \rangle$$

Other friezes generated by two symmetries

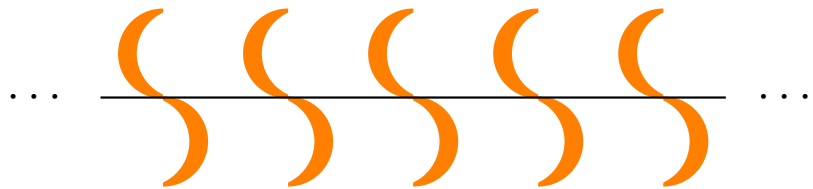
Frieze 3: eliminate the vertical flip and all rotations

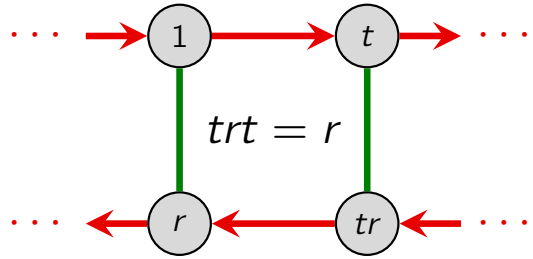




$$\mathbf{Frz}_3 = \{t^i \mid i \in \mathbb{Z}\} \cup \{h_j \mid j \in \mathbb{Z}\} = \langle t, h \mid h^2 = 1,\ tht = h \rangle$$

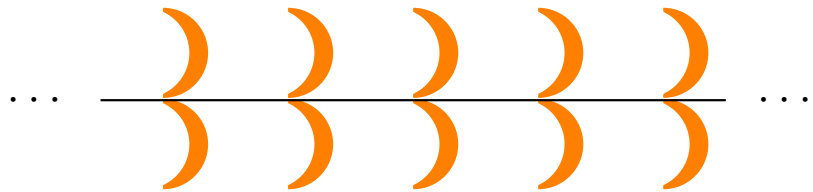
Frieze 4: eliminate the vertical flip and all horizontal flips

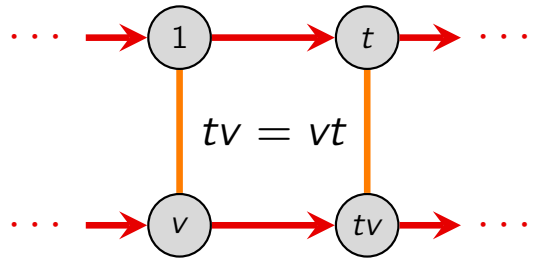




$$\mathbf{Frz}_4 = \{t^i \mid i \in \mathbb{Z}\} \cup \{r_j \mid j \in \mathbb{Z}\} = \langle t, r \mid r^2 = 1,\ trt = r \rangle$$

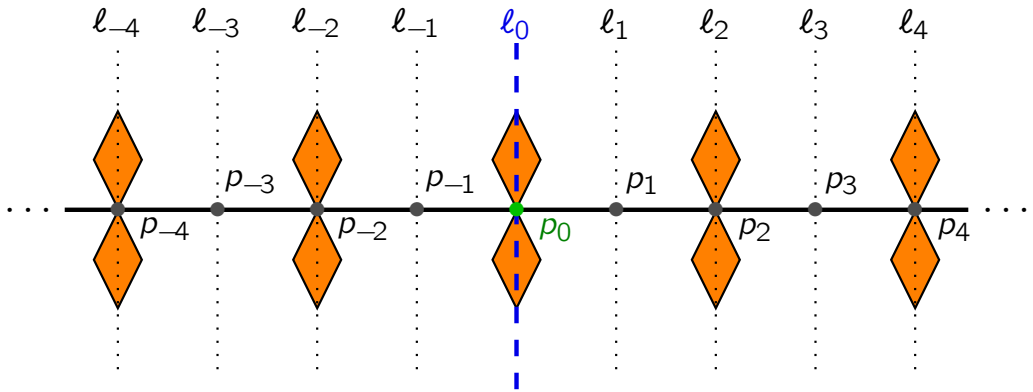
Frieze 5: eliminate all horizontal flips and rotations





$$\mathbf{Frz}_5 = \{t^i \mid i \in \mathbb{Z}\} \cup \{g_j \mid j \in \mathbb{Z}\} = \langle t, v \mid v^2 = 1,\ tv = vt \rangle$$

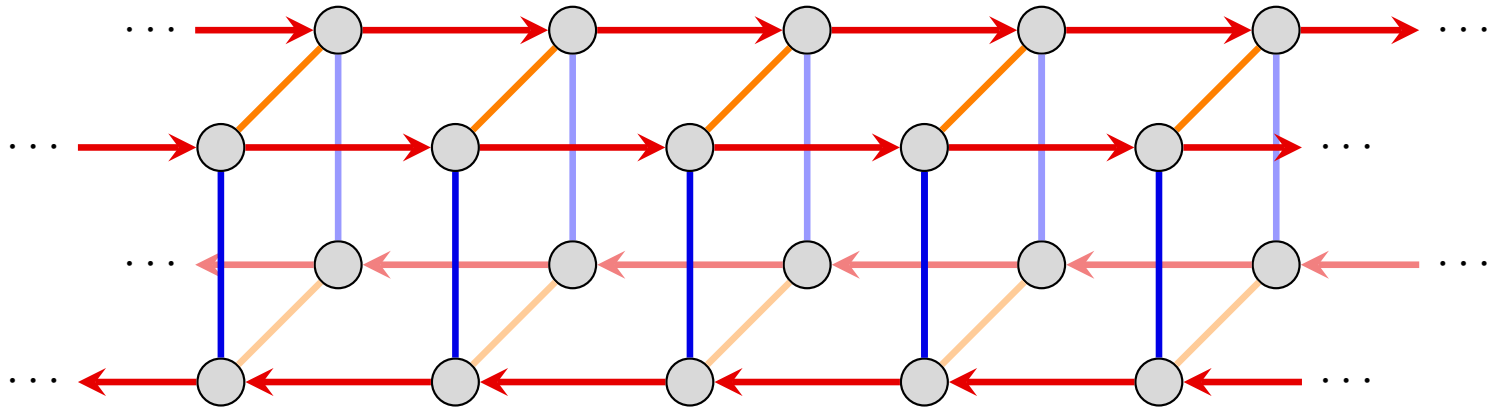
A Cayley graph of our first frieze group



A presentation for this frieze group is

$$\mathbf{Frz}_1 = \langle t, h, v \mid h^2 = v^2 = 1,\ hv = vh,\ tv = vt,\ tht = h \rangle.$$

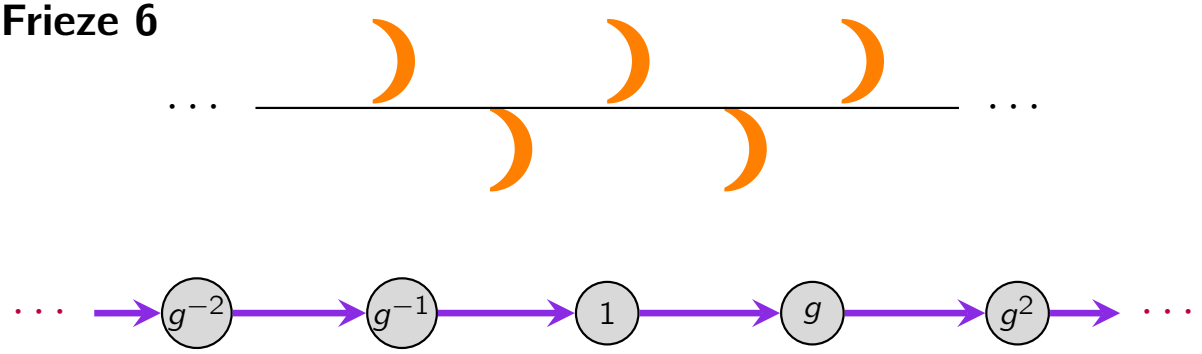
We can make a Cayley graph by piecing together the "tiles" on the previous slide:



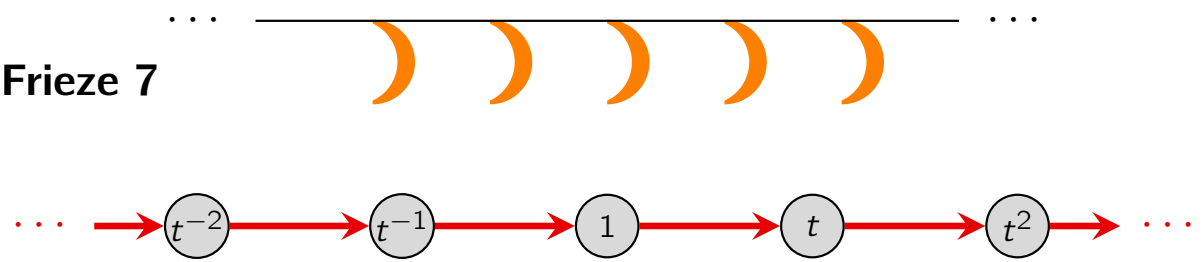
Classification of frieze groups

Since frieze groups are infinite, each one must contain a translation.

Frieze 6



Frieze 7



The frieze groups are $\mathbf{Frz}_6 = \langle g \mid \quad \rangle \cong \mathbf{Frz}_7 = \langle t \mid \quad \rangle$.

Theorem

There are 7 different frieze groups, but only 4 up to isomorphism.

Wallpaper and crystal groups

A frieze is a pattern than repeats in one dimension.

A next natural step is to look at discrete patterns that repeat in higher dimensions.

- a 2-dimensional repeating pattern is a wallpaper.
- a 3-dimensional repeating pattern is a crystal. The branch of mathematical chemistry that studies crystals is called crystallography.

In two dimensions, patterns can have 2-fold, 3-fold, 4-fold, or 6-fold symmetry.

Patterns can also have reflective symmetry, or be "chiral."

Symmetry groups of wallpapers are called wallpaper groups.

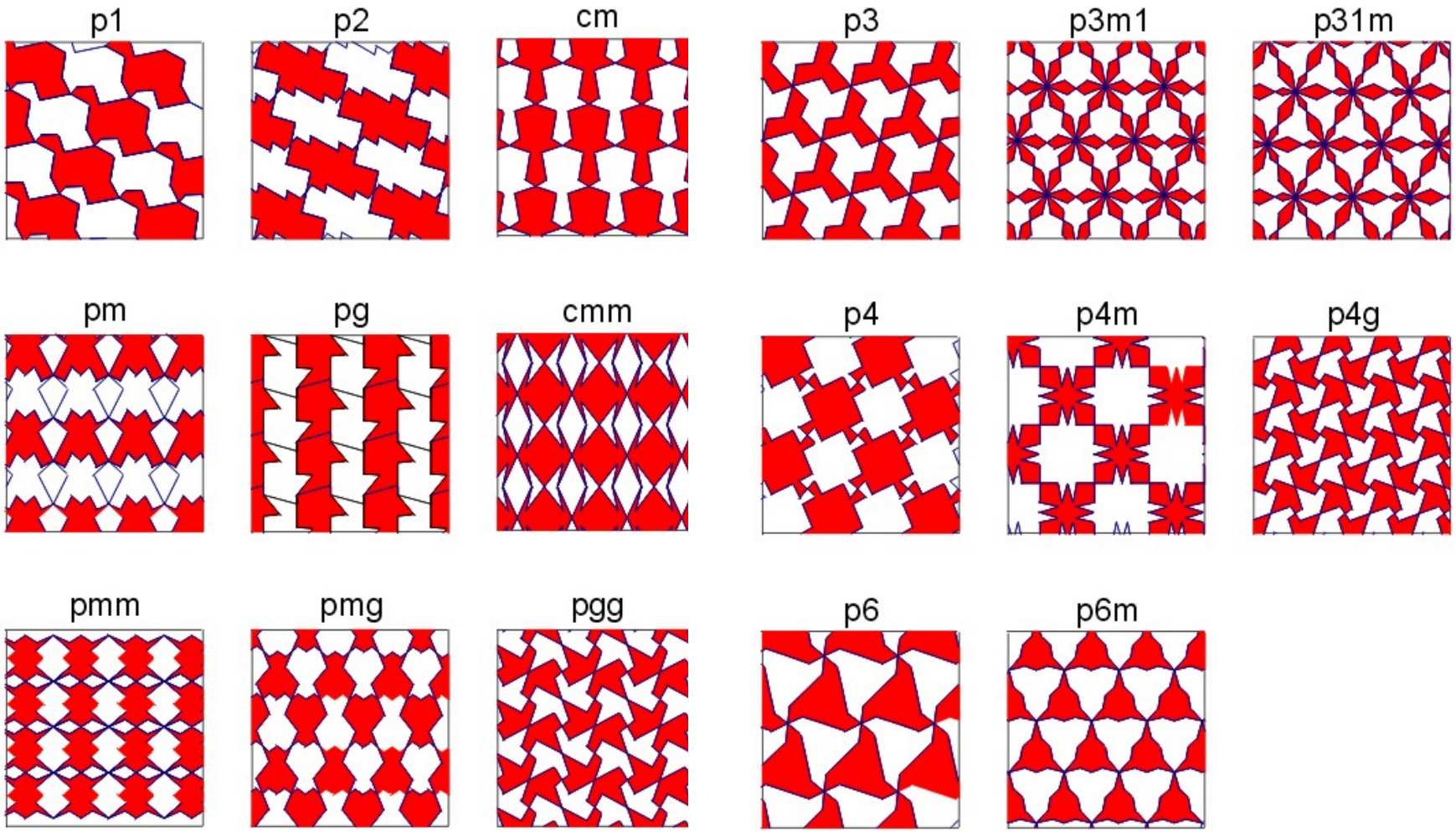
These were classified by Russian mathematician and crystallographer Evgraf Fedorov (1853–1919).

Theorem (1877)

There are 17 different wallpaper groups.

Mathematicians like to say "*there are only 17 different types of wallpapers*."

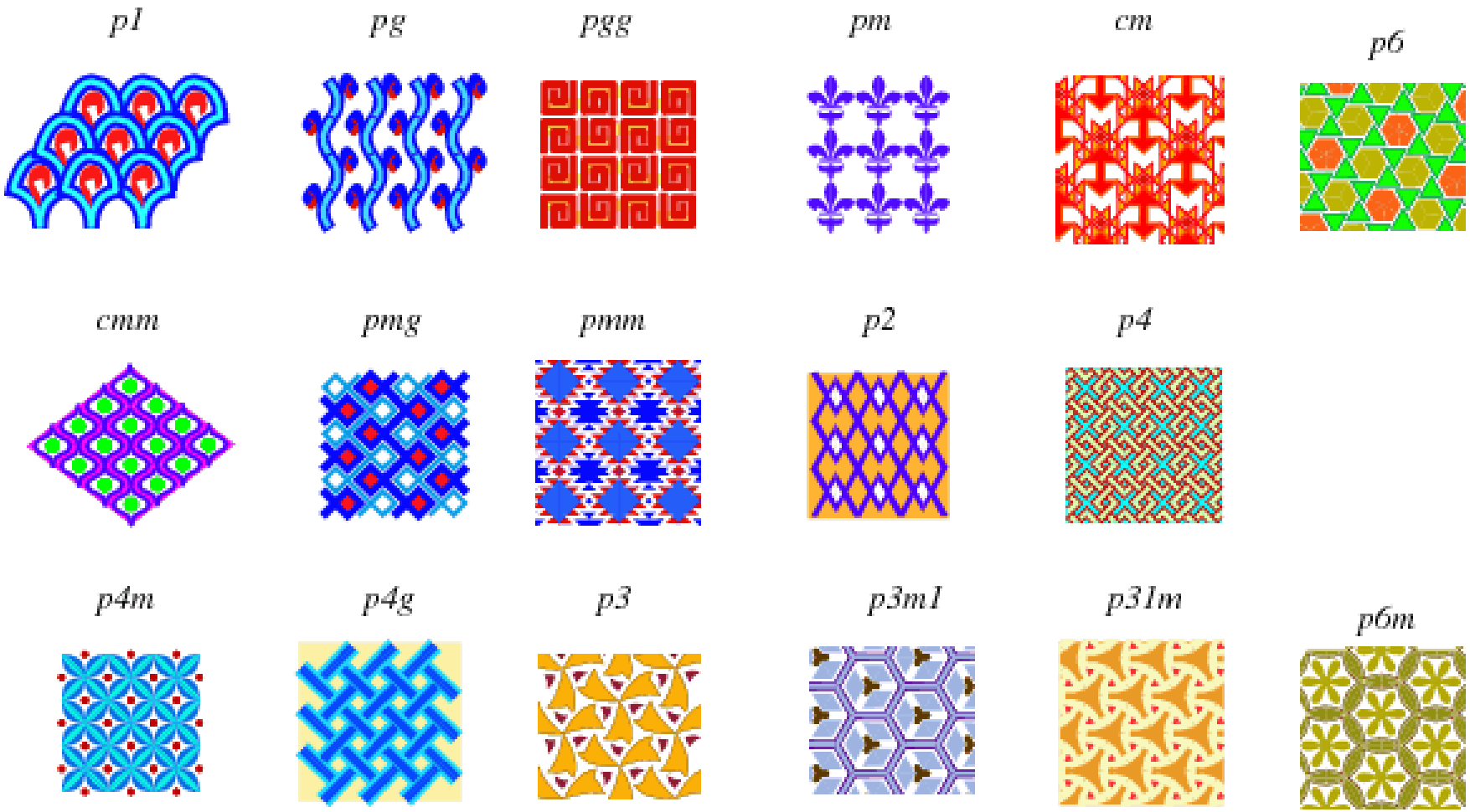
The 17 types of wallpaper patterns



Images by Patrick Morandi (New Mexico State University).

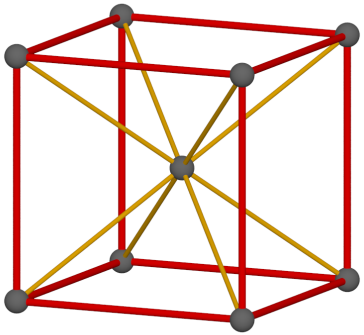
The 17 types of wallpaper patterns

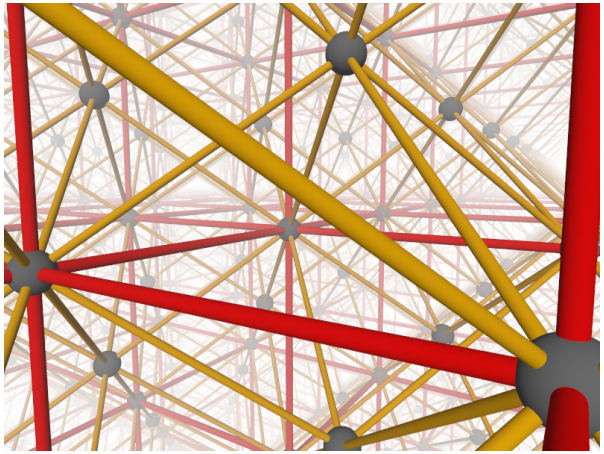
Here is another picture of all 17 wallpapers, with the official IUC notation for the symmetry group, adopted by the International Union of Crystallography in 1952.



Symmetry groups of crystals

Symmetry groups of crystals are called space, crystallographic, or Fedrov groups.





They were classified by Fedorov and Schöflies in 1892.

Theorem (1877)

There are 230 space groups.

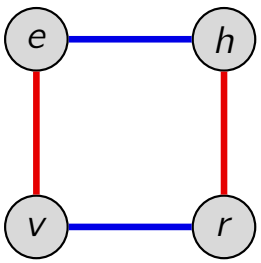
In 1978, a group of mathematicians showed there were exactly 4895 four-dimensional symmetry groups.

In 2002, it was discovered that two were actually the same, so there's only 4894.

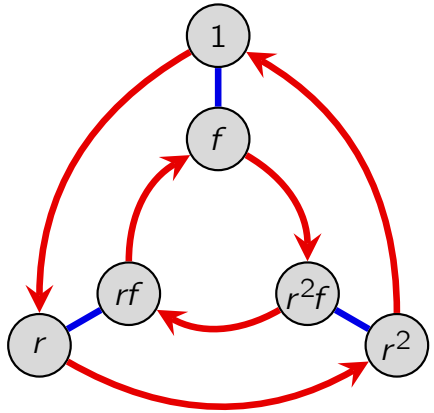
Cayley tables

In somes sense, a Cayley graph is a type of "group calculator."

Another useful tool is something we all learned about in grade school.



	e	v	h	r
e	e	v	h	r
v	v	e	r	h
h	h	r	e	v
r	r	h	v	e



	1	r	r^2	f	rf	r^2f
1	1	r	r^2	f	rf	r^2f
r	r	r^2	1	rf	r^2f	f
r^2	r^2	1	r	r^2f	f	rf
f	f	r^2f	rf	1	r^2	r
rf	rf	f	r^2f	r	1	r^2
r^2f	r^2f	rf	f	r^2	r	1

We will call this a Cayley table.

Notational convention

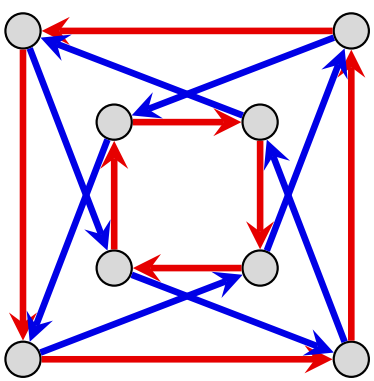
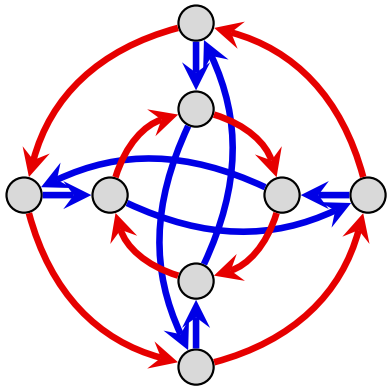
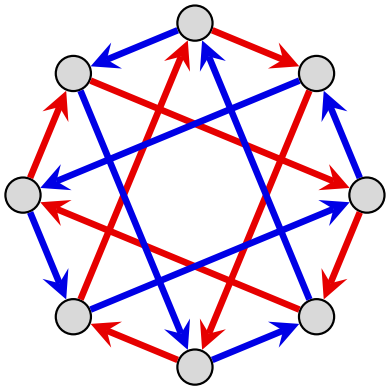
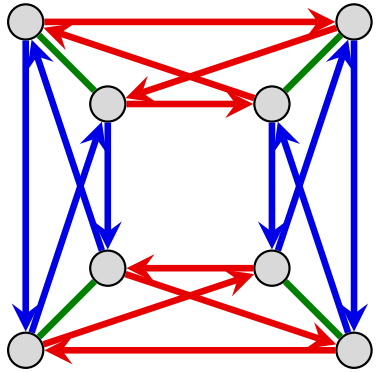
Since $ab \neq ba$ in general, we will say that the entry in row a and column b is ab.

Cayley tables can reveals patterns that are otherwise hidden.

Sometimes, these patterns only appear if we arrange elements in a certain order.

The quaternion group

Here are four Cayley graphs of a new group called the quaternion group, Q_8.

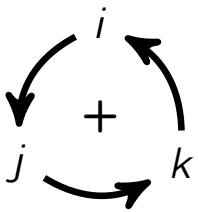





It's in no way clear that these even represent isomorphic groups.

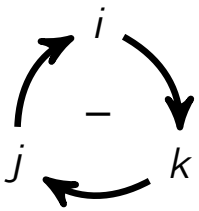
Notice how each one highlights different structural properties.

The first two Cayley graphs emphasize similarities and differences between Q_8 and **Sq**.

The group Q_8 is generated by "imaginary numbers" i, j, k, with $i^2 = j^2 = k^2 = -1$.



multiplying in this direction
yields a positive result



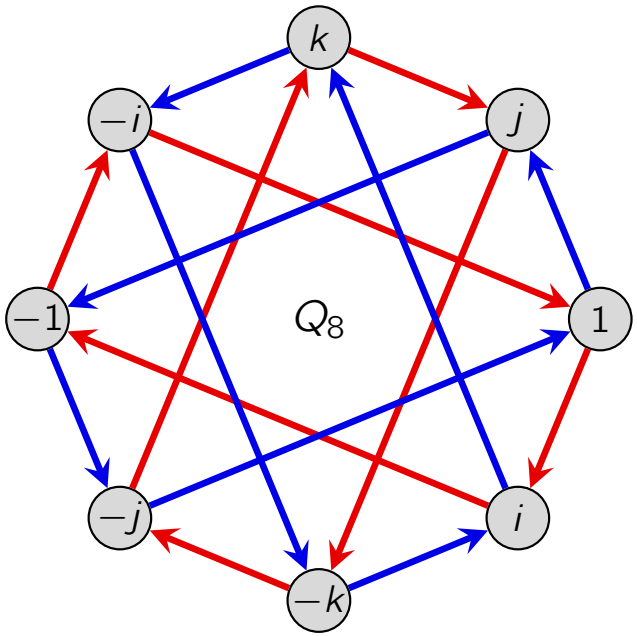
multiplying in this direction
yields a negative result

The quaternion group

Two possible presentations for the quaternions are

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle = \langle i, j \mid i^4 = j^4 = 1,\ iji = j \rangle .$$

This is one case where it's convenient to *not* use a minimal generating set.



	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

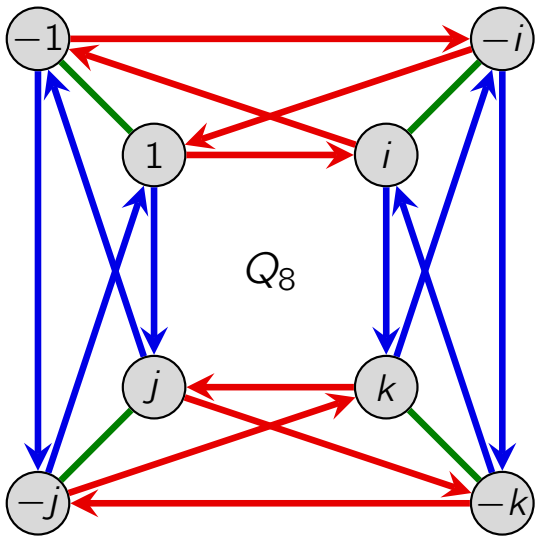
Remember how we said that some patterns in Cayley tables only appear if we arrange elements in a certain order?

The quaternion group

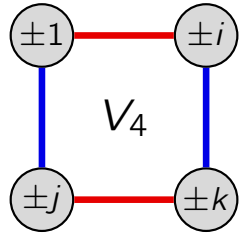
Rather than order elements as $1, i, j, k, -1, -i, -j, -k$ in

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle = \langle i, j \mid i^4 = j^4 = 1,\ iji = j \rangle,$$

let's construct a Cayley table with them ordered $1, -1, i, -i, j, -j, k, -k$.



	1	−1	i	$-i$	j	$-j$	k	$-k$
1	1	−1	i	$-i$	j	$-j$	k	$-k$
−1	−1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	−1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	−1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	−1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	−1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	−1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	−1



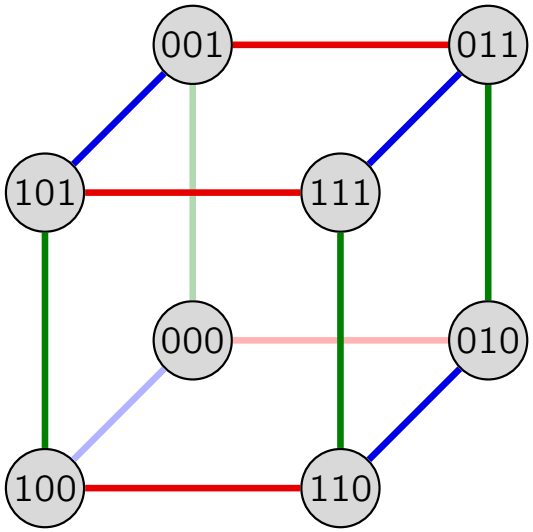
	±1	±i	±j	±k
±1	±1	±i	±j	±k
±i	±i	±1	±k	±j
±j	±j	±k	±1	±i
±k	±k	±j	±i	±1

Remark

"Collapsing" the group $Q_8 = \{\pm 1, \pm i, \pm j \pm k\}$ in this manner reveals the structure of V_4!

This is an example of taking a quotient of a group by a subgroup. We'll return to this!

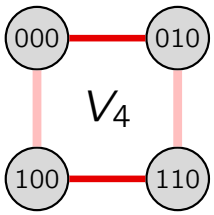
Another example of a quotient: $\mathbf{Light}_3$



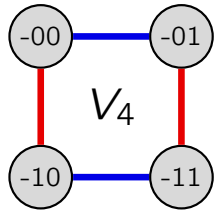
	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

"*subgroup of* $\mathbf{Light}_3$

	000	100	010	110
000	000	100	010	110
100	100	000	110	010
010	010	110	000	100
110	111	010	100	000



"*quotients of* $\mathbf{Light}_3$



	-00	-10	-01	-11
-00	-00	-10	-01	-11
-10	-10	-00	-11	-01
-01	-01	-11	-00	-10
-11	-11	-01	-10	-00

	--0	--1
--0	--0	--1
--1	--1	--0

Cayley tables

Proposition

An element cannot appear twice in the same row or column of a multiplication table.

Proof

Suppose that in row a, the element g appears in columns b and c. Algebraically, this means

$$ab = g = ac.$$

Multiplying everything on the left by a^{-1} yields

$$a^{-1}ab = a^{-1}g = a^{-1}ac \qquad \Longrightarrow \qquad b = c.$$

Thus, g (or any element) element cannot appear twice in the same row.

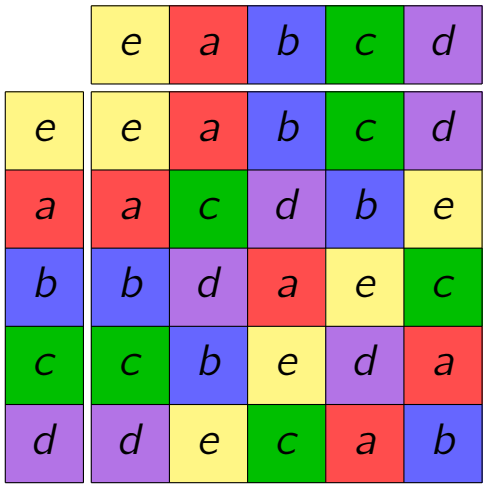
Verifying that g cannot appear twice in the same column is analogous. (Exercise) □

Question. *If we have a table where every element appears in every row and column once, is it a Cayley table for some group?*

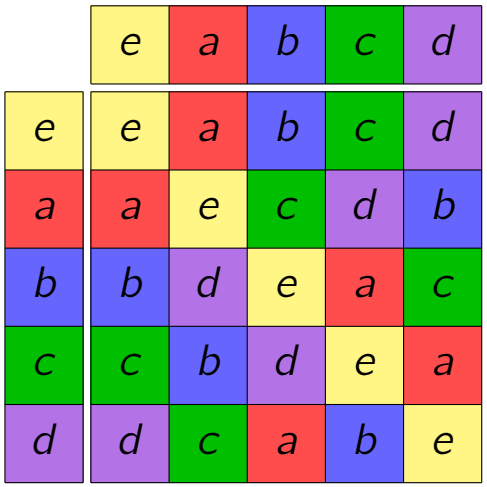
Latin squares and forbidden Cayley tables

A table where every element appears in every row and column once is called a Latin square.

Here is an example of two Latin square on a set of five elements, with identity element e.



	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b



	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Exploratory exercise

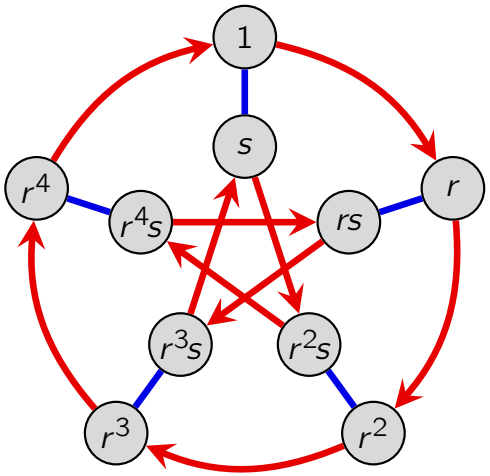
Can you construct a Cayley graph for either of these Latin squares? If not, what goes wrong?

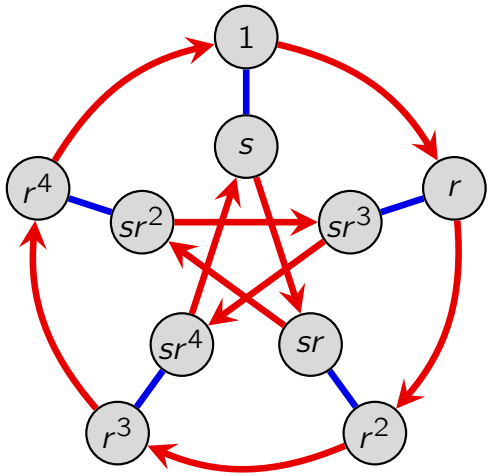
Forbidden Cayley graphs

Motivated by symmetries, we began by calling members of a group "actions"

Then we encountered Q_8, and it wasn't clear that there even is an underlying action.

It is natural to ask: *Can we use a Cayley graph to define an abstract group?*





Consider $r^2s = sr$, and the blue-red path. This takes 10 iterations from any node to return.

But that would imply that $G = \langle sr \rangle$, and every cyclic group must be abelian. *(Why?)*

As before, we can try to write a presentation from this graph:

$$G = \langle r, s \mid r^5 = s^2 = 1,\ rs = sr^3,\ r^2s = sr,\ r^3s = sr^4,\ r^4s = sr^2 \rangle$$

Question. *What group is this?*

Binary operations and associativity

The last few slides are a cautionary tale for why we need a formal definition.

A group is a set of elements satisfying a few properties.

Combining elements can be done with a binary operation, e.g., $+$, $-$, $\cdot$, and $\div$.

Definition

If $*$ is a binary operation on a set S, then $s * t \in S$ for all $s, t \in S$. In this case, we say that S is closed under the operation $*$.

Alternatively, we say that $*$ is a binary operation on S.

Definition

A binary operation $*$ on S is associative if

$$a * (b * c) = (a * b) * c, \qquad \text{for all } a, b, c \in S.$$

Associative basically means *parentheses are permitted anywhere, but required nowhere*.

For example, addition and multiplication are associative, but subtraction is not:

$$4 - (1 - 2) \neq (4 - 1) - 2.$$

The formal definition of a group

We are now ready to formally define a group.

Definition

A group is a set G satisfying the following properties:

1. There is an associative binary operation $*$ on G.
2. There is an identity element $e \in G$. That is, $e * g = g = g * e$ for all $g \in G$.
3. Every element $g \in G$ has an inverse, g^{-1}, satisfying $g * g^{-1} = e = g^{-1} * g$.

Remarks

- Depending on context, the binary operation may be denoted by $*$, $\cdot$, $+$, or $\circ$.
- We frequently omit the symbol and write, e.g., xy for $x * y$.
- We only use $+$ if G is abelian. Thus, $g + h = h + g$ (always), but in general, $gh \neq hg$.
- Uniqueness of the identity and inverses is *not* built into this definition. However, it's an easy exercise to establish.

A few simple properties

Let's verify uniqueness of the identity and inverses.

Theorem

Every element of a group has a unique inverse.

Verification

Let g be an element of a group G. By definition, it has at least one inverse.

Suppose that h and k are both inverses of g. This means that $gh = hg = e$ and $gk = kg = e$. It suffices to show that $h = k$. Indeed,

$$h = he = h(gk) = (hg)k = ek = k\,,$$

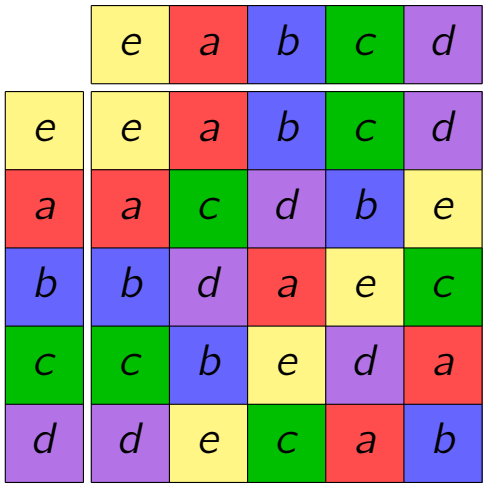
which is what we needed to show. □

The following is relegated to the homework; the technique is similar.

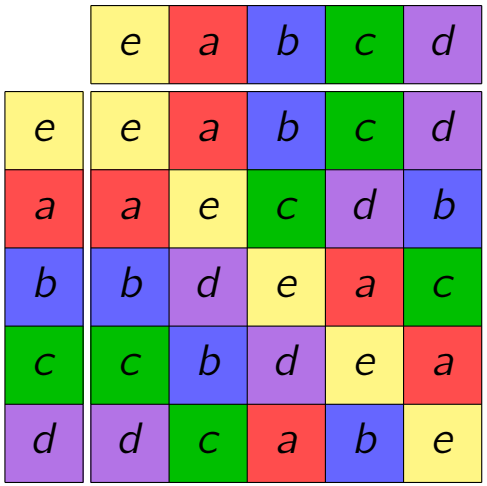
Theorem

Every group has a unique identity element.

Revisiting our Latin squares



	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b



	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

The table left describes a group $\mathbb{Z}_5 := \{0, 1, 2, 3, 4\}$ under addition modulo 5:

$$e = 0, \qquad a = 1, \qquad b = 3, \qquad c = 2, \qquad d = 4.$$

The table on the right fails associativity:

$$(a * b) * d = c * d = a, \qquad a * (b * d) = a * c = d.$$

Due to *F.W. Light's associativity test*, there is no shortcut for determining whether the binary operation in a Latin square is associative.

Specifically, the worst-case running time is $O(n^3)$, the number of (a, b, c)-triples.