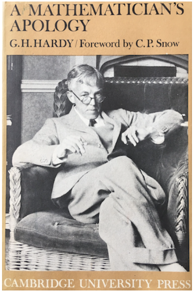
Chapter 1: Groups, intuitively

Matthew Macauley

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

Math 8510, Graduate 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."*

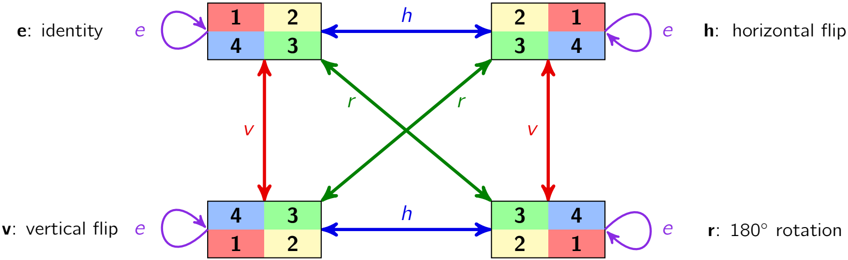
Very few mathematical fields embody visual patterns as well as group theory.

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

Symmetries of a rectangle

The group $V_4 = \{e, h, v, r\}$ of symmetries of a rectangle is called the **Klein** 4-**group**, named after German mathematician Felix Klein (1849–1925).

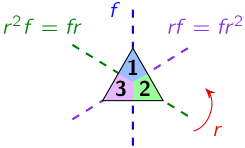
We can visualize it by a **Cayley graph**, named after British mathematician Arthur Cayley (1821–1895).

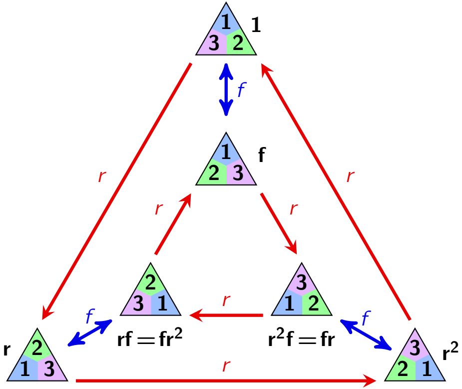


Symmetries of a triangle

Here is a Cayley graph for the **dihedral group** $D_3 = \langle r, f \rangle$.

This group is nonabelian (order matters!), and we will read from *left-to-right*.





Equalities like the following are called relations:

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

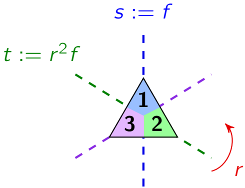
A different generating set for the symmetries of the triangle

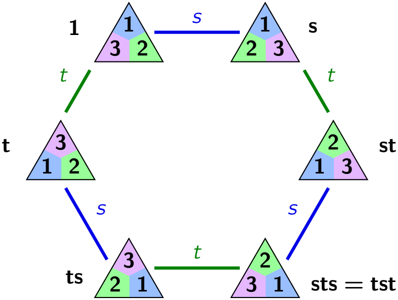
Recall that the triangle symmetry group is $D_3 = \{\underbrace{1,\ r,\ r^2}_{\text{rotations}},\ \underbrace{f,\ rf,\ r^2 f}_{\text{reflections}}\}$.

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

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

Here is a Cayley graph corresponding to $D_3 = \langle s, t\rangle$, where $s := f$ and $t := r^2 f = fr$.



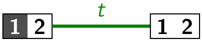


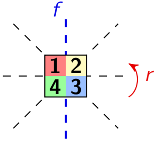
Henceforth, we will draw bidirected arrows as *undirected*.

Three groups of size 8

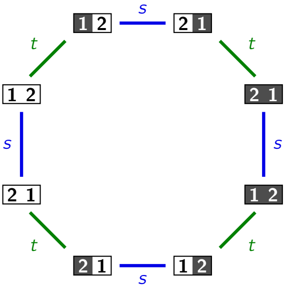
Consider the following groups, where one uses the following operations:

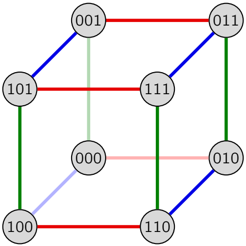
- s: swap the two squares
- t: toggle the color of the first square.

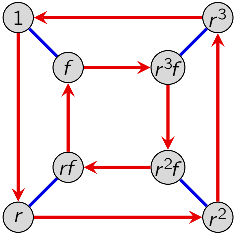




Question: *Do any of these groups have the same structure? (Are they "isomorphic"?)*

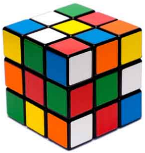
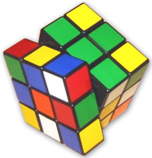
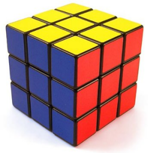






The Rubik's cube group

One of the most famous groups is the set of legal moves of the Rubik's Cube.

Theorem (2014)

There are 43,252,003,274,489,856,000 distinct configurations of the Rubik's cube. Each one can be reached from the solved state in at most

- 20 moves, in the "standard metric"
- 26 moves, in the "quarter turn metric."

This toy was invented in 1974 by architect Ernő Rubik of Budapest, Hungary.

His Wikipedia page used to say:

> *He is known to be a very introverted and hardly accessible person, almost impossible to contact or get for autographs.*

A famous toy

Not impossible . . . just almost impossible.

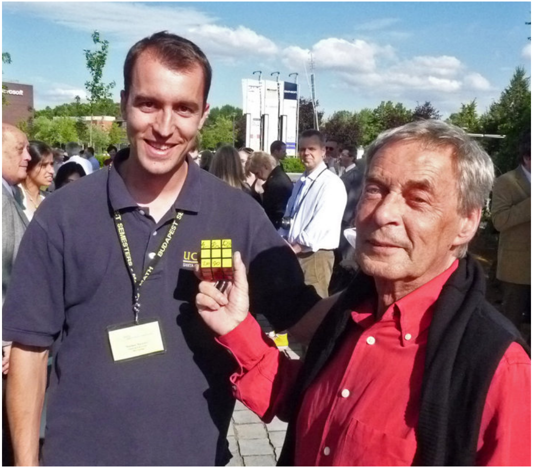
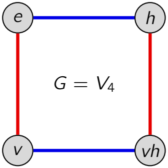


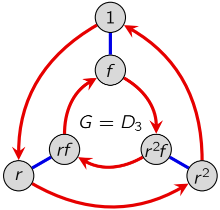
Figure: June 2010, in Budapest, Hungary

Group presentations

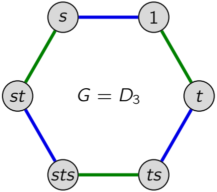
We can use a presentation to describe a group by its generators and relations.



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



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

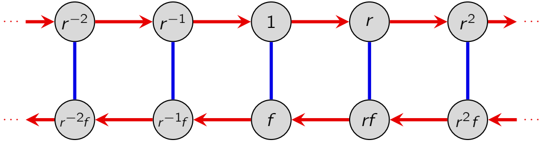


$\langle s, t \mid s^2 = t^2 = 1,\ sts = tst \rangle$

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

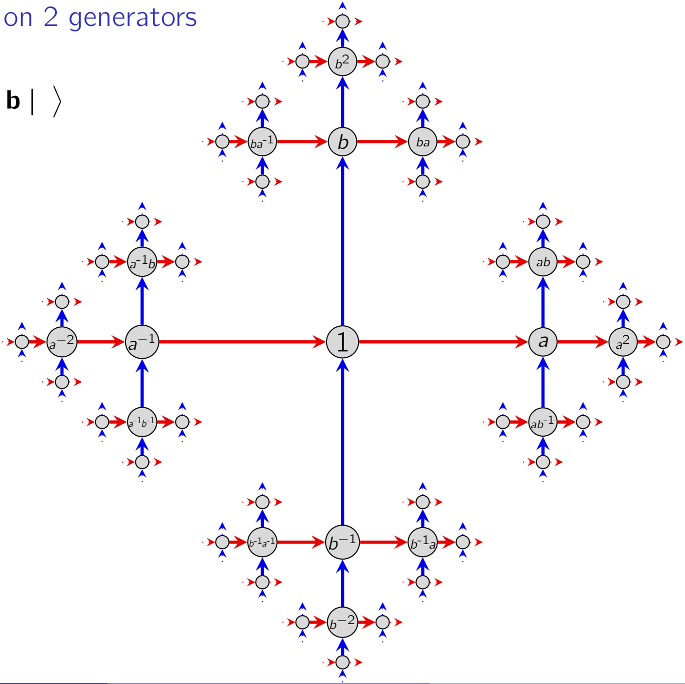
$$rf = fr^2 \quad \Rightarrow \quad f(rf) = r^2 \quad \Rightarrow \quad (frf)^2 = r^4 \quad \Rightarrow \quad fr^2f = r^4 \quad \Rightarrow \quad (fr^2)f = r^4$$
$$\Rightarrow \quad (rf)f = r^4 \quad \Rightarrow \quad r = r^4 \quad \Rightarrow \quad 1 = r^3$$

But removing $r^3 = 1$ from $D_3 = \langle r, f \mid r^3 = f^2 = 1,\ rf = fr^{-1} \rangle$ yields an infinite group.



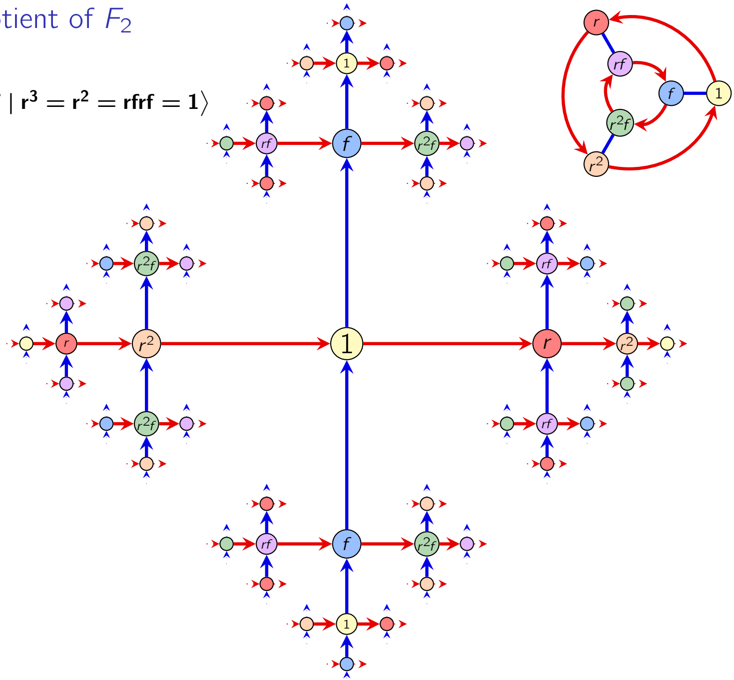
The free group on 2 generators

$$\mathbf{F_2} = \langle \mathbf{a}, \mathbf{b} \mid \; \rangle$$



D_3 as a quotient of F_2

$$\mathbf{D_3} = \langle \mathbf{r}, \mathbf{f} \mid \mathbf{r}^3 = \mathbf{r}^2 = \mathbf{rfrf} = \mathbf{1} \rangle$$



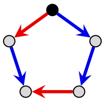
The word problem

The word problem

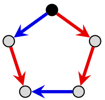
Given a presentation $G = \langle g_1, \dots, g_n \mid r_1 = e, \dots, r_m = e \rangle$, is $G = \{e\}$?

Exercise

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



and



$\Longrightarrow$

$aba^{-1}b^{-2} = 1$ $\quad$ $bab^{-1}a^{-2} = 1$ $\quad$ $G = \langle a, b, \mid a = b = 1 \rangle = \langle 1 \rangle$

An even harder problem is the isomorphism problem: Given G_1, 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)

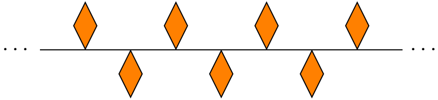
Frieze groups

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.

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



Definition

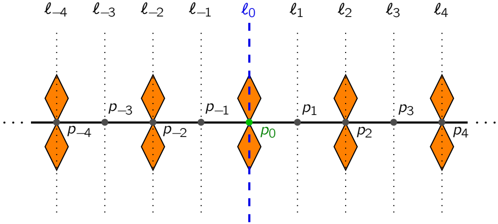
The symmetry group of a frieze is called a frieze group.

Goal. *Understand and classify the frieze groups.*

Frieze groups

Every symmetry of a frieze is one of the following:

- vertical reflection (unique!)
- horizontal reflection
- 180° rotation
- translation
- glide-reflection



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

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

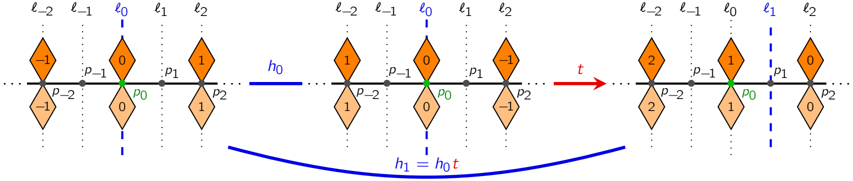
Note that $v = g_0$. Letting $h := h_0$, $r := r_0$, and $g := g_1$, this frieze group is generated by

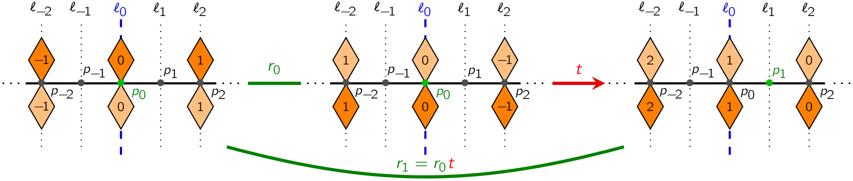
$$\mathbf{Frz}_1 := \langle t, h, v \rangle = \langle t, h, r \rangle = \langle t, v, r \rangle = \langle g, h, v \rangle = \cdots$$

The other frieze groups are all subgroups of $\mathbf{Frz}_1$.

Frieze groups

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

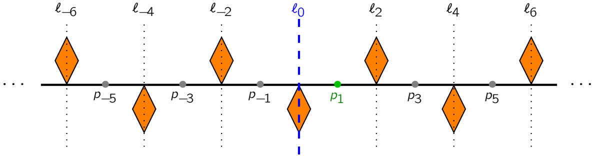




Similarly, it follows that $h_i t = h_{i+1}$ and $r_i t = r_{i+1}$ for any $i \in \mathbb{Z}$.

A "smaller" frieze group

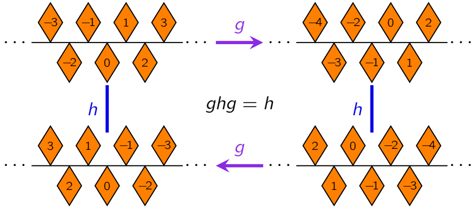
Let's eliminate the vertical symmetry from the previous frieze group.

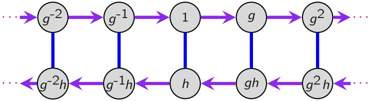


We lose half of the horizontal reflections and rotations in the process. The frieze group is

$$\mathbf{Frz}_2 := \{g_i \mid i \in \mathbb{Z}\} \cup \{h_{2j} \mid j \in \mathbb{Z}\} \cup \{r_{2k+1} \mid k \in \mathbb{Z}\} = \langle g, h \rangle = \langle vt, h \rangle = \langle g, r_1 \rangle = \langle vt, rt \rangle.$$

To find a presentation, we just have to see how $g := g_1 = tv$ and h are related:

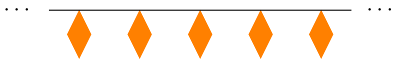


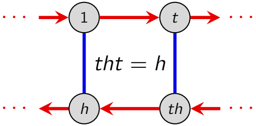


$$\mathbf{Frz}_2 = \langle g, h \mid h^2 = 1,\ ghg = h \rangle$$

Other friezes generated by two symmetries

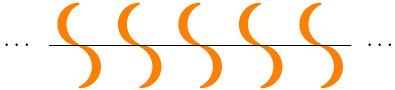
Frieze 3: eliminate the vertical flip and all rotations

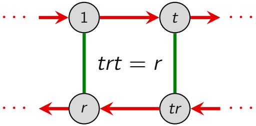




$$\mathbf{Frz}_3 = \{t^i \mid i \in \mathbb{Z}\} \cup \{h_j \mid j \in \mathbb{Z}\} = \langle t, h \mid h^2 = 1,\ tht = h \rangle$$

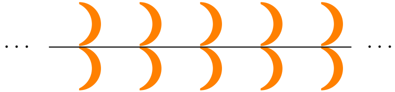
Frieze 4: eliminate the vertical flip and all horizontal flips

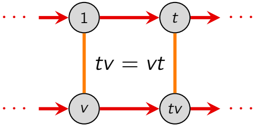




$$\mathbf{Frz}_4 = \{t^i \mid i \in \mathbb{Z}\} \cup \{r_j \mid j \in \mathbb{Z}\} = \langle t, r \mid r^2 = 1,\ trt = r \rangle$$

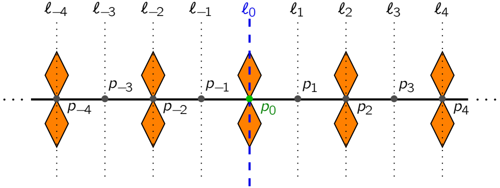
Frieze 5: eliminate all horizontal flips and rotations





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

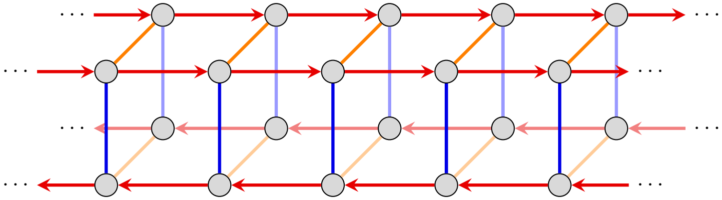
A Cayley graph of our first frieze group



A presentation for this frieze group is

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

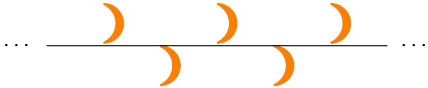
We can make a Cayley graph by piecing together the "tiles" on the previous slide:

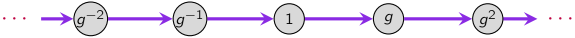


Classification of frieze groups

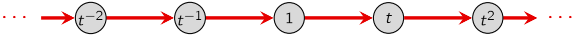
Since frieze groups are infinite, each one must contain a translation.

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.

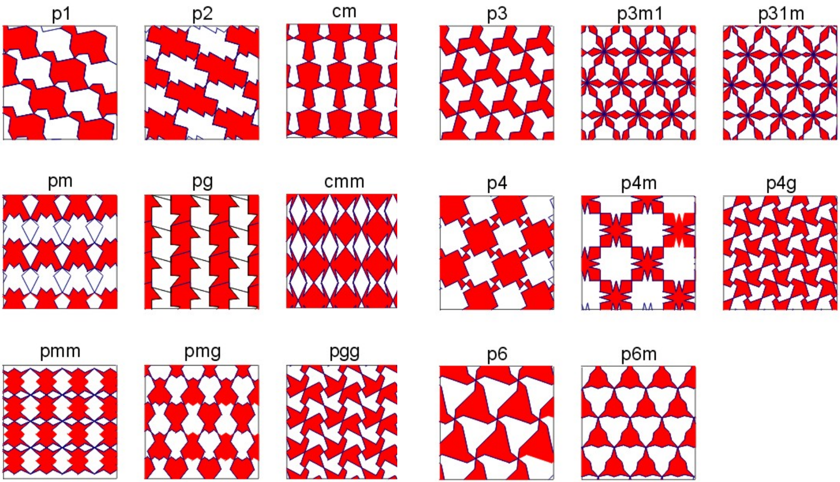
These were classified by Russian mathematician and crystallographer Evgraf Fedorov (1853–1919).

Theorem (1877)

There are 17 different wallpaper groups.

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

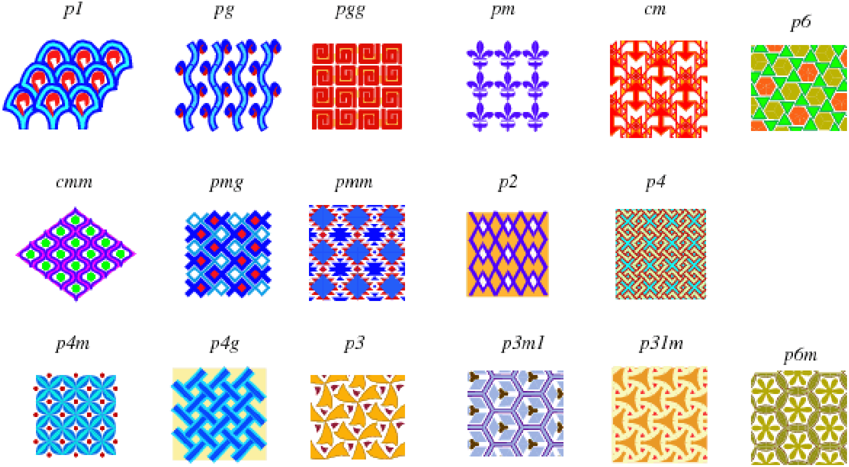
The 17 types of wallpaper patterns



Images by Patrick Morandi (New Mexico State University).

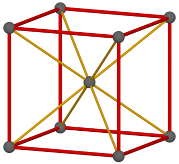
The 17 types of wallpaper patterns

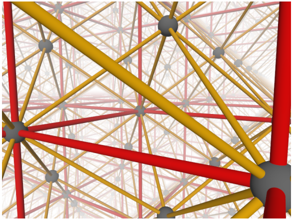
Here is another picture of all 17 wallpapers, with the official IUC notation for the symmetry group, adopted by the International Union of Crystallography in 1952.



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.

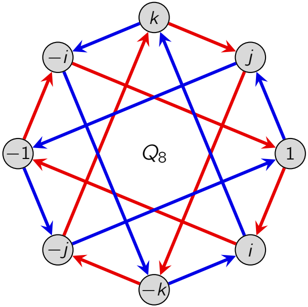
The quaternion group

A Cayley table can be used to quickly multiply group elements.

Here is an example, for a new group called the quaternions:

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

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

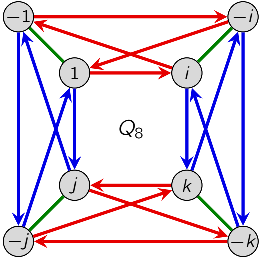
Certain patterns in Cayley tables only appear if we arrange elements in a certain order.

The quaternion group

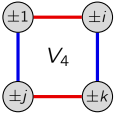
Rather than order elements as $1, i, j, k, -1, -i, -j, -k$ in

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

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



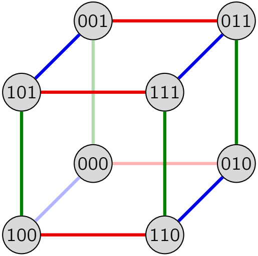
	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1



	± 1	$\pm i$	$\pm j$	$\pm k$
± 1	± 1	$\pm i$	$\pm j$	$\pm k$
$\pm i$	$\pm i$	± 1	$\pm k$	$\pm j$
$\pm j$	$\pm j$	$\pm k$	± 1	$\pm i$
$\pm k$	$\pm k$	$\pm j$	$\pm i$	± 1

We say that V_4 is a quotient of Q_8.

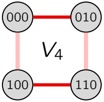
Another example of a quotient: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$



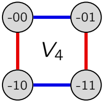
	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001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

“*subgroup of* $\mathbb{Z}_2^3$

	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* $\mathbb{Z}_2^3$

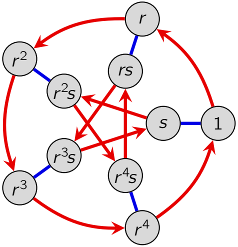


	-00	-10	-01	-11
-00	-00	-10	-01	-11
-10	-10	-00	-11	-01
-01	-01	-11	-00	-10
-11	-11	-01	-10	-00

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

Why we need a formal definition

Do you see why neither of the following define a group?



	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

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. It is associative if

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

The Latin square on the right fails associativity:

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

The formal definition of a group

Due to *F.W. Light's associativity test*, there is no shortcut for determining a 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.

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 $g * g^{-1} = e = g^{-1} * g$.

Exercise

Let G be a group. Then:

- Every element has a unique inverse.
- The identity element is unique.