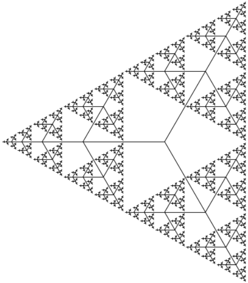
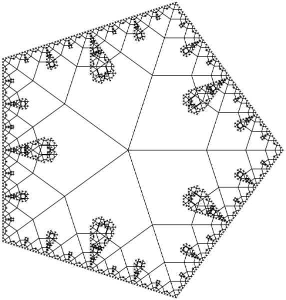
Free Groups and Infinite Trees



with

Noah Luntzlara

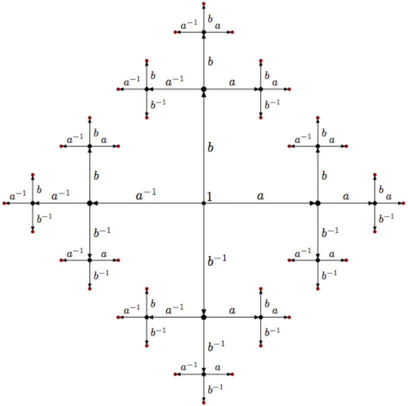
November 21, 2018



Honors 135.004
Fractals: Their Beauty and Topology
Connor Davis

Outline

- Group Theory
- Examples of Groups
- Free groups
- Cayley graphs



Group Theory

Group theory

Group theory

Group theory is the study of *symmetry*.

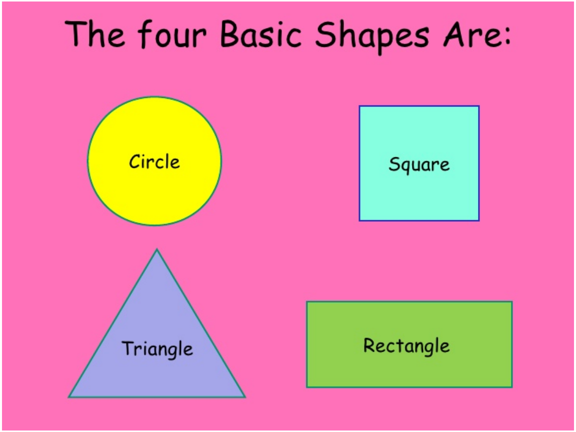
Group theory

Group theory

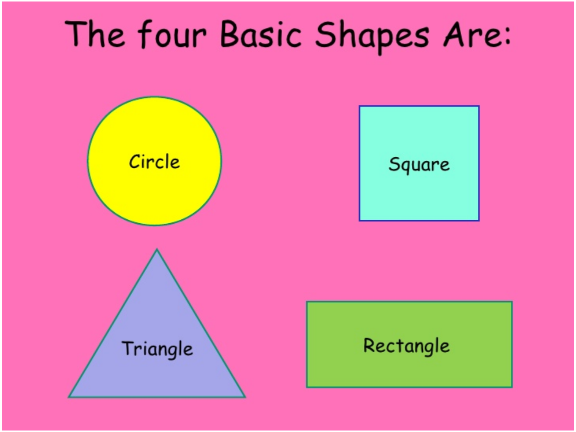
Group theory is the study of *symmetry*.

What is symmetry?

Symmetry


The four Basic Shapes Are:
Circle
Square
Triangle
Rectangle

Symmetry



Which is the most symmetric? Which is the least?

Symmetry

Definition

A *symmetry* is a transformation that leaves something unchanged.

Symmetry

Definition

A *symmetry* is a transformation that leaves something unchanged.

Symmetry

Definition

A *symmetry* is a transformation that leaves something unchanged.

- Symmetries are always *reversible*.
- *Doing nothing* is always a symmetry.

Groups

Symmetries describe something concrete about an object. A group, on the other hand is a set of abstract symmetries.

Groups

Symmetries describe something concrete about an object. A group, on the other hand is a set of abstract symmetries.

Definition

A *group* is a pair $(G, *)$, where G is a set and $*$ is a multiplication rule, which satisfies:

- **Associativity** $g * (h * k) = (g * h) * k$ always holds.
- There is an **identity** e in G such that for any g in G,
$$e * g = g \text{ and } g * e = g.$$
- Every g in G has an **inverse** g^{-1} in G such that
$$g * g^{-1} = e \text{ and } g^{-1} * g = e.$$

Examples of Groups

Examples of Groups

What are some examples of groups?

Examples of Groups

What are some examples of groups?

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
    - **Associativity.** $a + (b + c) = (a + b) + c$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.**

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.**

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Associativity.** $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Associativity.** $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.
  - **Identity.**

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Associativity.** $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.
  - **Identity.** $1 \cdot r = r \cdot 1 = r$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Associativity.** $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.
  - **Identity.** $1 \cdot r = r \cdot 1 = r$.
  - **Inverses.**

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

You can make groups out of numbers.

- $(\mathbb{Z}, +)$, where $\mathbb{Z}$ is integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
  - **Associativity.** $a + (b + c) = (a + b) + c$.
  - **Identity.** $0 + a = a + 0 = a$.
  - **Inverses.** $a + (-a) = (-a) + a = 0$.
- Same thing with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Associativity.** $r \cdot (s \cdot t) = (r \cdot s) \cdot t$.
  - **Identity.** $1 \cdot r = r \cdot 1 = r$.
  - **Inverses.** $0 \cdot (\text{anything}) = 0 \neq 1$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
    - **Inverses.** $0 \cdot (\text{anything}) = 0 \neq 1$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Inverses.** $0 \cdot (\text{anything}) = 0 \neq 1$.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R}, \cdot)$ is *not* a group!
  - **Inverses.** $0 \cdot (\text{anything}) = 0 \neq 1$.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.
  - **Inverses.** $r \cdot (1/r) = (1/r) \cdot r = 1$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$,

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$,

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, not $(\mathbb{Z} \setminus \{0\}, \cdot)$

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, not $(\mathbb{Z} \setminus \{0\}, \cdot)$, $\cdots$

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, not $(\mathbb{Z} \setminus \{0\}, \cdot)$, $\cdots$
- Matrix groups with matrix multiplication, like

  $GL_2(\mathbb{R}) = \{2 \cdot 2$ matrices, entries in $\mathbb{R}$ and $\det = 1\}$.

Groups of Numbers

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, not $(\mathbb{Z} \setminus \{0\}, \cdot)$, $\cdots$
- Matrix groups with matrix multiplication, like

  $GL_2(\mathbb{R}) = \{2 \cdot 2 \text{ matrices, entries in } \mathbb{R} \text{ and } \det = 1\}$.

N.B. For most pairs of matrices, $AB \neq BA$. For instance,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

So generally $g * h = h * g$ isn't true in any group.

Definition

A group $(G, *)$ is *abelian* provided that $g * h = h * g$ for any elements g, h in G.

Definition

A group $(G, *)$ is *abelian* provided that $g * h = h * g$ for any elements g, h in G.

The operation is then said to be *commutative*.

Definition

A group $(G, *)$ is *abelian* provided that $g * h = h * g$ for any elements g, h in G.

The operation is then said to be *commutative*.

Abelian groups.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\cdots$
- $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $\cdots$

Non-abelian groups.

- $GL_2(\mathbb{R})$.

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Theorem

The set of symmetries of any object where the operation is *composition* forms a group!

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Theorem

The set of symmetries of any object where the operation is *composition* forms a group!

Proof.

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Theorem

The set of symmetries of any object where the operation is *composition* forms a group!

Proof. Recall:

- Symmetries are always *reversible*.
- *Doing nothing* is always a symmetry.

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Theorem

The set of symmetries of any object where the operation is *composition* forms a group!

Proof. Recall:

- Symmetries are always *reversible*.
- *Doing nothing* is always a symmetry.

Thus we have **inverses**, **identity**.

Symmetry Groups

Associativity $g * (h * k) = (g * h) * k$.
Identity e such that $e * g = g * e = g$.
Inverses g^{-1} such that $g * g^{-1} = g^{-1} * g = e$.

Theorem

The set of symmetries of any object where the operation is *composition* forms a group!

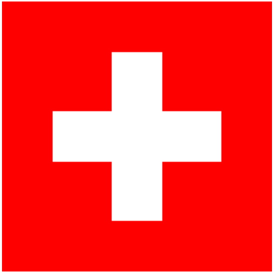
Proof. Recall:

- Symmetries are always *reversible*.
- *Doing nothing* is always a symmetry.

Thus we have **inverses**, **identity**. Furthermore, composition of transformations is **associative**.

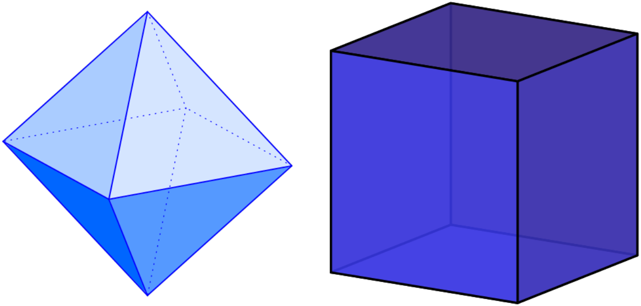
Symmetry Groups

What are the symmetry groups of these shapes?



Symmetry Groups

Amazing but true! These two objects have the same symmetry group:



Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

- Vector spaces (Linear groups)

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

- Vector spaces (Linear groups)
- Field extensions (Galois groups)

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

- Vector spaces (Linear groups)
- Field extensions (Galois groups)
- Manifolds (Mapping class groups)

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

- Vector spaces (Linear groups)
- Field extensions (Galois groups)
- Manifolds (Mapping class groups)
- L-functions (The modular group)

Symmetry in Mathematics

The greatest developments in modern math have come from studying symmetries of mathematical structures.

Some objects with important symmetry groups:

- Vector spaces (Linear groups)
- Field extensions (Galois groups)
- Manifolds (Mapping class groups)
- L-functions (The modular group)
- Spacetime (Lorentz group and Poincaré group)

Free Groups

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

$$w_1 = edcedc$$

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

$$w_1 = edcedc$$
$$w_2 = aaaaa = a^5$$

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

$$w_1 = edcedc$$
$$w_2 = aaaaa = a^5$$
$$w_3 = cabbage = cab^2age$$

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

$$w_1 = edcedc$$
$$w_2 = aaaaa = a^5$$
$$w_3 = cabbage = cab^2age$$
$$w_4 = f$$

Words

Definition

Let S be a set of symbols. A *word* in S is an ordered list of elements in S, not necessarily distinct.

Example. $S = \{a, b, c, d, e, f, g\}$

$$w_1 = edcedc$$
$$w_2 = aaaaa = a^5$$
$$w_3 = cabbage = cab^2age$$
$$w_4 = f$$
$$w_5 = \emptyset$$

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}.

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words may be *simplified* by deleting subwords of the form xx^{-1} or $x^{-1}x$. For instance, if $S = \{a, b, c\}$,

$$ab^3c^{-1}cb^{-1}c$$

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words may be *simplified* by deleting subwords of the form xx^{-1} or $x^{-1}x$. For instance, if $S = \{a, b, c\}$,

$$ab^3c^{-1}cb^{-1}c \to ab^3b^{-1}c$$

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words may be *simplified* by deleting subwords of the form xx^{-1} or $x^{-1}x$. For instance, if $S = \{a, b, c\}$,

$$ab^3c^{-1}cb^{-1}c \to ab^3b^{-1}c \to ab^2c.$$

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words may be *simplified* by deleting subwords of the form xx^{-1} or $x^{-1}x$. For instance, if $S = \{a, b, c\}$,

$$ab^3c^{-1}cb^{-1}c \to ab^3b^{-1}c \to ab^2c.$$

Definition

1. A word in $S \cup S^{-1}$ is *reduced* p.t. it can't be simplified.

Words

Let S be a set of symbols. For every symbol x in S, associate a corresponding symbol x^{-1}. Call the set of such symbols S^{-1}. Consider words in $S \cup S^{-1}$.

Words may be *simplified* by deleting subwords of the form xx^{-1} or $x^{-1}x$. For instance, if $S = \{a, b, c\}$,

$$ab^3c^{-1}cb^{-1}c \to ab^3b^{-1}c \to ab^2c.$$

Definition

1. A word in $S \cup S^{-1}$ is *reduced* p.t. it can't be simplified.
2. Two words are *equivalent* p.t. they can be simplified to the same reduced word.

Concatenation

Definition

Concatenation is the operation $\circ$ on words which places the symbols of one word after the other.

Concatenation

Definition

Concatenation is the operation $\circ$ on words which places the symbols of one word after the other.

Example. $w_1 = iam, w_2 = sam$

Concatenation

Definition

Concatenation is the operation $\circ$ on words which places the symbols of one word after the other.

Example. $w_1 = iam, w_2 = sam$

$$w_1 \circ w_2 = iamsam$$
$$w_2 \circ w_1 = samiam$$

Concatenation

Definition

Concatenation is the operation $\circ$ on words which places the symbols of one word after the other.

Example. $w_1 = iam, w_2 = sam$

$$w_1 \circ w_2 = iamsam$$
$$w_2 \circ w_1 = samiam$$

N.B. concatenation is not commutative!

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a\}$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a\}$

$$F_S = \{\ldots, a^{-2}, a^{-1}, \emptyset, a, a^2, \ldots\}$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a\}$

$$F_S = \{\ldots, a^{-2}, a^{-1}, \emptyset, a, a^2, \ldots\}$$

$$a^m \circ a^n = a^{m+n}$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a\}$

$$F_S = \{\dots, a^{-2}, a^{-1}, \emptyset, a, a^2, \dots\}$$

$$a^m \circ a^n = a^{m+n}$$

$$(F_S, \circ) \cong (\mathbb{Z}, +)$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

$$aba^2ba^{-1} \circ ab^{-1}a^{-1}ba^{-1}b^2 =$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set S* is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

$$aba^2ba^{-1} \circ ab^{-1}a^{-1}ba^{-1}b^2 = aba^2ba^{-1}ab^{-1}a^{-1}ba^{-1}b^2$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

$$\begin{aligned} aba^2ba^{-1} \circ ab^{-1}a^{-1}ba^{-1}b^2 &= aba^2b\color{red}{a^{-1}a}b^{-1}a^{-1}ba^{-1}b^2 \\ &= aba^2\color{red}{bb^{-1}}a^{-1}ba^{-1}b^2 \end{aligned}$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set S* is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

$$\begin{aligned} aba^2ba^{-1} \circ ab^{-1}a^{-1}ba^{-1}b^2 &= aba^2b\color{red}{a^{-1}a}\color{black}{b^{-1}a^{-1}ba^{-1}b^2} \\ &= aba^2\color{red}{bb^{-1}}\color{black}{a^{-1}ba^{-1}b^2} \\ &= ab\color{red}{a^2a^{-1}}\color{black}{ba^{-1}b^2} \end{aligned}$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

Example. $S = \{a, b\}$

$$
\begin{aligned}
aba^2ba^{-1} \circ ab^{-1}a^{-1}ba^{-1}b^2 &= aba^2b{\color{red}a^{-1}a}b^{-1}a^{-1}ba^{-1}b^2 \\
&= aba^2{\color{red}bb^{-1}}a^{-1}ba^{-1}b^2 \\
&= ab{\color{red}a^2a^{-1}}ba^{-1}b^2 \\
&= {\color{blue}ababa^{-1}b^2}.
\end{aligned}
$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

N.B. F_S depends only on the number of generators $|S|$.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

N.B. F_S depends only on the number of generators $|S|$.

Thus the (finitely generated) free groups are $F_1, F_2, F_3, \ldots$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$:

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$: $\emptyset \circ w = w \circ \emptyset = w$.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$: $\emptyset \circ w = w \circ \emptyset = w$.
Inverses.

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$: $\emptyset \circ w = w \circ \emptyset = w$.
Inverses. $g = a_1 \cdots a_k$,

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$: $\emptyset \circ w = w \circ \emptyset = w$.
Inverses. $g = a_1 \cdots a_k$, $g^{-1} = a_k^{-1} \cdots a_1^{-1}$

Free Group

Definition

The *free group* $(F_S, \circ)$ on *generating set* S is the group of non-equivalent words in $S \cup S^{-1}$, where $\circ$ is the concatenation operation.

We check that the free group is a group.

Associativity. Word concatenation is associative:

$$w_1 \circ (w_2 \circ w_2) = a_1 \cdots a_j b_1 \cdots b_k c_1 \cdots c_\ell = (w_1 \circ w_2) \circ w_2$$

Identity. $e = \emptyset$: $\emptyset \circ w = w \circ \emptyset = w$.
Inverses. $g = a_1 \cdots a_k$, $g^{-1} = a_k^{-1} \cdots a_1^{-1}$

$$a_1 \cdots a_k \circ a_k^{-1} \cdots a_1^{-1} = a_k^{-1} \cdots a_1^{-1} \circ a_1 \cdots a_k = e.$$

Relations

We impose *relations* $r_1, r_2, \ldots, r_k$ in F_S on a free group by declaring

$$r_1 = r_2 = \cdots = r_k = e,$$

and following through all the implications.

Relations

We impose *relations* $r_1, r_2, \ldots, r_k$ in F_S on a free group by declaring

$$r_1 = r_2 = \cdots = r_k = e,$$

and following through all the implications.

Example. The *free abelian group* $\mathbb{Z}_S$ from F_S by setting

$$aba^{-1}b^{-1} = e$$

for every pair of generators a, b.

Relations

We impose *relations* $r_1, r_2, \ldots, r_k$ in F_S on a free group by declaring

$$r_1 = r_2 = \cdots = r_k = e,$$

and following through all the implications.

Example. The *projective special linear group*

Relations

We impose *relations* $r_1, r_2, \ldots, r_k$ in F_S on a free group by declaring

$$r_1 = r_2 = \cdots = r_k = e,$$

and following through all the implications.

Example. The *projective special linear group* $\mathrm{PSL}(2, \mathbb{Z})$ from $F_{\{s,t\}}$ by

$$s^2 = (st)^3 = e.$$

Relations

We impose *relations* $r_1, r_2, \ldots, r_k$ in F_S on a free group by declaring

$$r_1 = r_2 = \cdots = r_k = e,$$

and following through all the implications.

Example. The *projective special linear group* $\mathrm{PSL}(2, \mathbb{Z})$ from $F_{\{s,t\}}$ by

$$s^2 = (st)^3 = e.$$

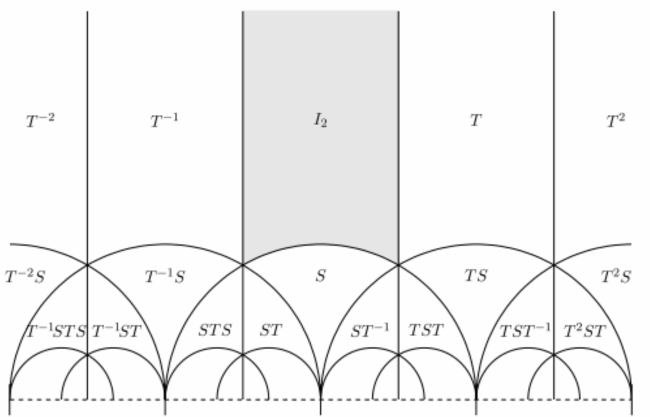
$\mathrm{PSL}(2, \mathbb{Z})$ can be realized as symmetries on the upper half plane $\mathbb{H}^2 = \{x + iy \in \mathbb{C} : x > 0\}$ formed by

$$S : z \mapsto -1/z, \qquad T : z \mapsto z + 1$$

$\mathbf{PSL}(2,\mathbb{Z})$

$\mathrm{PSL}(2,\mathbb{Z})$ can be realized as symmetries on the upper half plane $\mathbb{H}^2 = \{x + iy \in \mathbb{C} : x > 0\}$ formed by

$$S : z \mapsto -1/z, \qquad T : z \mapsto z + 1$$



Presentations

Definition

A *presentation* of a group is a way of writing it as a free group with relations.

Presentations

Definition

A *presentation* of a group is a way of writing it as a free group with relations.

Theorem

Every group has a presentation!

Presentations

Definition

A *presentation* of a group is a way of writing it as a free group with relations.

Theorem

Every group has a presentation!

The Word Problem

Given a presentation of a group, and two words w_1, w_2, how can you tell if they are equal in the group?

The Word Problem

The Word Problem

Given a presentation of a group G with finitely many relations $r_1, \ldots, r_k$ and two words w_1, w_2 written in the generators, how can you tell if they are equal in G?

The Word Problem

The Word Problem

Given a presentation of a group G with finitely many relations $r_1, \ldots, r_k$ and two words w_1, w_2 written in the generators, how can you tell if they are equal in G?

Example. In $\mathrm{PSL}(2, \mathbb{Z})$ [$= F_{\{s,t\}}$ with $s^2 = (st)^3 = e$]

The Word Problem

The Word Problem

Given a presentation of a group G with finitely many relations $r_1, \ldots, r_k$ and two words w_1, w_2 written in the generators, how can you tell if they are equal in G?

Example. In $\mathrm{PSL}(2, \mathbb{Z})$ [$= F_{\{s,t\}}$ with $s^2 = (st)^3 = e$],

$$sts = t^{-1}st^{-1}$$

The Word Problem

The Word Problem

Given a presentation of a group G with finitely many relations $r_1, \ldots, r_k$ and two words w_1, w_2 written in the generators, how can you tell if they are equal in G?

Example. In $\mathrm{PSL}(2, \mathbb{Z})$ [$= F_{\{s,t\}}$ with $s^2 = (st)^3 = e$],

$$sts = t^{-1}st^{-1}$$

Theorem

There is no algorithm which can solve the word problem.

Cayley Graphs

Cayley Graphs

Definition

Given a group G and a presentation with generators S, its *Cayley graph* is the graph with the elements of G as vertices and edges $g - (s * g)$ if s is a generator.

Cayley Graphs

Definition

Given a group G and a presentation with generators S, its *Cayley graph* is the graph with the elements of G as vertices and edges $g - (s * g)$ if s is a generator.

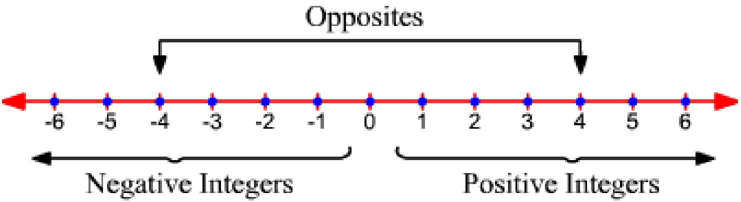
Example. $G = (\mathbb{Z}, +)$, $S = \{1\}$.

Cayley Graphs

Definition

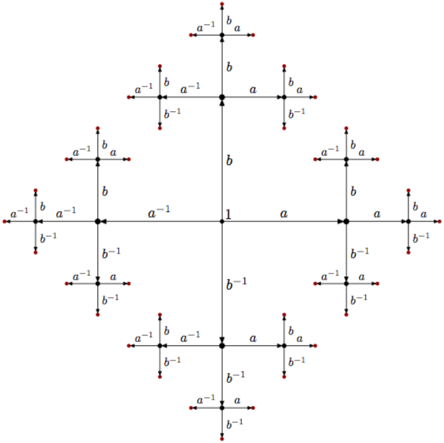
Given a group G and a presentation with generators S, its *Cayley graph* is the graph with the elements of G as vertices and edges $g - (s * g)$ if s is a generator.

Example. $G = (\mathbb{Z}, +)$, $S = \{1\}$.



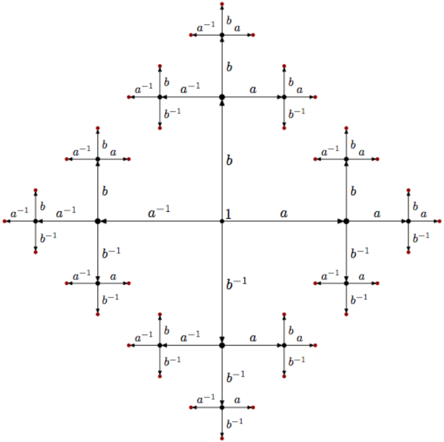
Cayley Graphs

Example. The free group F_2 on 2 generators.



Cayley Graphs

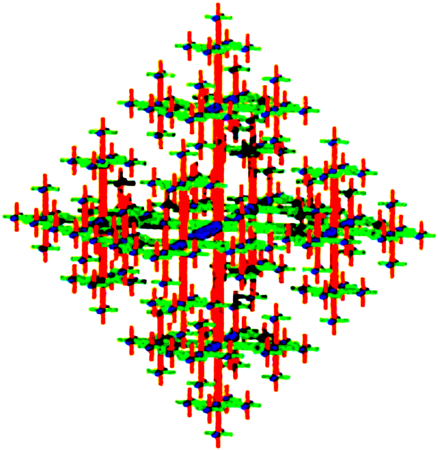
Example. The free group F_2 on 2 generators.



This graph is used in the proof of the Banach-Tarski theorem.

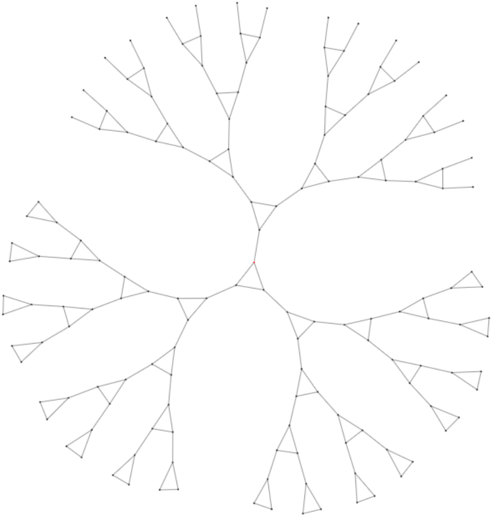
Cayley Graphs

Example. The free group F_3 on 3 generators.



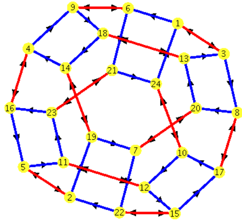
Cayley Graphs

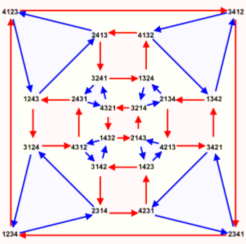
Example. PSL$(2, \mathbb{Z})$ with generators $\{s, t\}$.

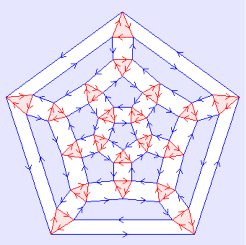


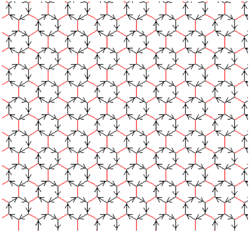
Cayley Graphs

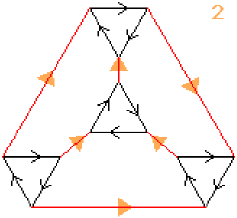
Some random Cayley Graphs

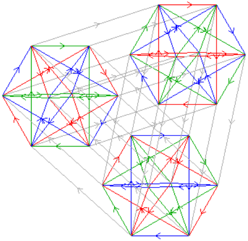












The End