Think of permutations as **vertices of a graph**.

Two vertices are connected by an edge if there is a permitted transition (according to bell ringers) that transforms one change into the other. Here what it looks like for 4 bells:
Hamiltonian cycle

- An extent is a path in this graph, visiting each of the vertices exactly once, and returning to the beginning vertex. Such tours are called Hamiltonian cycles.
- For Plain Bob, this path looks like that:
Let $G$ be a group, and let $S$ be a generating set of elements.

**Definition**

Let $\text{Cay}(G, S)$ be the colored directed graph having $G$ as the set of vertices, and for any $s \in S$ there is an edge going from $g$ to $gs$, and any such edge is colored into a unique color $c_s$ corresponding to $s \in S$.

- Draw Cayley graphs for $\mathbb{Z}$ with $S_1 = \{1\}$, and with $S_2 = \{2, 3\}$.
- Do the same for $\mathbb{Z}/6$ and $S = \{1\}$. 
Let $G$ be a group, and let $S$ be a generating set of elements.

**Definition**

Let $\text{Cay}(G, S)$ be the colored directed graph having $G$ as the set of vertices, and for any $s \in S$ there is an edge going from $g$ to $gs$, and any such edge is colored into a unique color $c_s$ corresponding to $s \in S$.

- Draw Cayley graphs for $\mathbb{Z}$ with $S_1 = \{1\}$, and with $S_2 = \{2, 3\}$.
- Do the same for $\mathbb{Z}/6$ and $S = \{1\}$.
- How about $\mathbb{Z}/3 \times \mathbb{Z}/2$ with $S = \{(1, 0), (0, 1)\}$?
Let $G$ be a group, and let $S$ be a generating set of elements.

**Definition**

Let $\text{Cay}(G, S)$ be the colored directed graph having $G$ as the set of vertices, and for any $s \in S$ there is an edge going from $g$ to $gs$, and any such edge is colored into a unique color $c_s$ corresponding to $s \in S$.

- Draw Cayley graphs for $\mathbb{Z}$ with $S_1 = \{1\}$, and with $S_2 = \{2, 3\}$.
- Do the same for $\mathbb{Z}/6$ and $S = \{1\}$.
- How about $\mathbb{Z}/3 \times \mathbb{Z}/2$ with $S = \{(1, 0), (0, 1)\}$?
- $D_4$ with generators $r_{90}$ (rotation by $90^\circ$) and $s_h$ (vertical reflection)?
Properties of Cayley graphs

- Prove that any Cayley graph is connected (if we ignore the orientation of edges).
Properties of Cayley graphs

- Prove that any Cayley graph is connected (if we ignore the orientation of edges).
- Between any two vertices $g, h$ there is at most one edge.
Properties of Cayley graphs

- Prove that any Cayley graph is connected (if we ignore the orientation of edges).
- Between any two vertices $g, h$ there is at most one edge.
- All vertices have the same degrees.
Properties of Cayley graphs

- Prove that any Cayley graph is connected (if we ignore the orientation of edges).
- Between any two vertices $g, h$ there is at most one edge.
- All vertices have the same degrees.
- What do (un-oriented) cycles in Cayley graphs mean?
• Prove that any Cayley graph is connected (if we ignore the orientation of edges).
• Between any two vertices $g, h$ there is at most one edge.
• All vertices have the same degrees.
• What do (un-oriented) cycles in Cayley graphs mean?
• Any group acts on its Cayley graph, sending a vertex corresponding to $h$ to the vertex corresponding to $gh$. 
Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph.

**Question (Mr. Drix):** how to see group multiplication from it?

Double the graph: for each edge add another one going in the opposite direction. Call the resulting graph $\tilde{\Gamma}$.

Or, equivalently, forget the orientation of edges at all.

Let $\hat{P}_\Gamma$ be the set of paths in $\tilde{\Gamma}$.

Let $\tilde{G}$ be the set of equivalence classes of elements in $\hat{P}_\Gamma$ starting at the vertex $e$, where two paths are called equivalent iff they differ by (oriented) cycles.
Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph.

**Question (Mr. Drix):** how to see group multiplication from it?

1. Double the graph: for each edge add another one going in the opposite direction. Call the resulting graph $\tilde{\Gamma}$.
2. Or, equivalently, forget the orientation of edges at all.
3. Let $P_\Gamma$ be the set of paths in $\tilde{\Gamma}$.
4. Let $\tilde{G}$ be the set of equivalence classes of elements in $P_\Gamma$ starting at the vertex $e$, where two paths are called equivalent iff they differ by (oriented) cycles.
Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph.

**Question (Mr. Drix):** how to see group multiplication from it?

2. Double the graph: for each edge add another one going in the opposite direction. Call the resulting graph $\widetilde{\Gamma}$.

3. Or, equivalently, forget the orientation of edges at all.
1. Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph.

**Question (Mr. Drix):** how to see group multiplication from it?

2. Double the graph: for each edge add another one going in the opposite direction. Call the resulting graph $\tilde{\Gamma}$.

3. Or, equivalently, forget the orientation of edges at all.

4. Let $P_\Gamma$ be the set of paths in $\tilde{\Gamma}$. 
Let $\Gamma = \text{Cay}(G, S)$ be a Cayley graph.

**Question (Mr. Drix):** how to see group multiplication from it?

Double the graph: for each edge add another one going in the opposite direction. Call the resulting graph $\tilde{\Gamma}$.

Or, equivalently, forget the orientation of edges at all.

Let $P_\Gamma$ be the set of paths in $\tilde{\Gamma}$.

Let $\tilde{G}$ be the set of equivalence classes of elements in $P_\Gamma$ starting at the vertex $e$, where two paths are called equivalent iff they differ by (oriented) cycles.
Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.

Let's define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$. Let $a_0 \in [a]$ be a path starting at the vertex $e \in G$, and ending at $g_0$. Pick a path $b_0$ from the class $[b]$ ending at $h_0$. It's given by a sequence $e, s_i^1, s_i^1 s_i^2, \ldots, s_i^1 s_i^2 \ldots s_i^r = h_0$. We then define $[a] \ast [b]$ to be the equivalence class of the composite path, first going along $a_0$, then continuing as $g_0 s_i^1, g_0 s_i^1 s_i^2$, etc. all the way up to $g_0 h_0$.

Claim: $\tilde{G}$ with the multiplication $\ast$ is a group, and is isomorphic to $G$. 

Sasha Patotski (Cornell University)
Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.

Let’s define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$. 

Claim: $\tilde{G}$ with the multiplication $\ast$ is a group, and is isomorphic to $G$. 

Sasha Patotski (Cornell University)  
Cayley graphs. Normal subgroups  
December 21, 2015 7 / 13
Group from its Cayley graph

- Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let’s define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$.
- Let $a_0 \in [a]$ be a path starting at the vertex $e \in G$, and ending at $g_0$. 

Sasha Patotski (Cornell University)  
Cayley graphs. Normal subgroups  
December 21, 2015  7 / 13
Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.

Let’s define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$.

Let $a_0 \in [a]$ be a path starting at the vertex $e \in G$, and ending at $g_0$.

Pick a path $b_0$ from the class $[b]$ ending at $h_0$.
It’s given by a sequence $e, s_{i_1}, s_{i_1} s_{i_2}, \ldots, s_{i_1} s_{i_2} \cdots s_{i_r} = h_0$. 
Group from its Cayley graph

- Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let's define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$.
- Let $a_0 \in [a]$ be a path starting at the vertex $e \in G$, and ending at $g_0$.
- Pick a path $b_0$ from the class $[b]$ ending at $h_0$.
  It's given by a sequence $e, s_{i_1}, s_{i_1}s_{i_2}, \ldots, s_{i_1}s_{i_2}\ldots s_{i_r} = h_0$.
- We then define $[a] \ast [b]$ to be the equivalence class of the composite path, first going along $a_0$, then continuing as $g_0s_{i_1}, g_0s_{i_1}s_{i_2}$ etc. all the way up to $g_0h_0$.

Claim: $\tilde{G}$ with the multiplication $\ast$ is a group, and is isomorphic to $G$. 

Sasha Patotski (Cornell University) 
Cayley graphs. Normal subgroups 
December 21, 2015
Let $\tilde{G}$ be the set of equivalence classes of paths in $\tilde{\Gamma}$ starting at the vertex $e$, where two paths are called equivalent iff they differ by some (oriented) cycles.

Let’s define multiplication on $\tilde{G}$. Take two equivalence classes of paths, say $[a]$ and $[b]$.

Let $a_0 \in [a]$ be a path starting at the vertex $e \in G$, and ending at $g_0$.

Pick a path $b_0$ from the class $[b]$ ending at $h_0$. It’s given by a sequence $e, s_{i_1}, s_{i_1}s_{i_2}, \ldots, s_{i_1}s_{i_2}\ldots s_{i_r} = h_0$.

We then define $[a] \ast [b]$ to be the equivalence class of the composite path, first going along $a_0$, then continuing as $g_0s_{i_1}$, $g_0s_{i_1}s_{i_2}$ etc. all the way up to $g_0h_0$.

**Claim:** $\tilde{G}$ with the multiplication $\ast$ is a group, and is isomorphic to $G$. 
**Claim:** $\tilde{G}$ with the multiplication $\ast$ is a group, and is isomorphic to $G$.

$\tilde{G}$ has identity and inverse obviously but not clearly associative.

Let's define a map $\tilde{G} \to G$ sending equivalence class $[a]$ to the end-point of its representative. This is well-defined: the end-point doesn't depend on the choice. This is obviously a homomorphism, and it's clearly surjective. It's also injective, so we get an isomorphism.

Done.
Claim: \( \tilde{G} \) with the multiplication \( \ast \) is a group, and is isomorphic to \( G \).

\( \tilde{G} \) has identity and inverse obviously but not clearly associative.

Let’s define a map \( \tilde{G} \to G \) sending equivalence class \([a]\) to the end-point of it’s representative.
Claim: \( \tilde{G} \) with the multiplication \( \ast \) is a group, and is isomorphic to \( G \).

\( \tilde{G} \) has identity and inverse obviously but not clearly associative.

Let’s define a map \( \tilde{G} \rightarrow G \) sending equivalence class \([a]\) to the end-point of it’s representative.

This is well-defined: the end-point doesn’t depend on the choice.
Claim: \( \tilde{G} \) with the multiplication \(*\) is a group, and is isomorphic to \( G \).
\( \tilde{G} \) has identity and inverse obviously but not clearly associative.
Let’s define a map \( \tilde{G} \to G \) sending equivalence class \([a]\) to the end-point of it’s representative.
This is well-defined: the end-point doesn’t depend on the choice.
This is obviously a homomorphism, and it’s clearly surjective.
Claim: \( \tilde{G} \) with the multiplication \( \ast \) is a group, and is isomorphic to \( G \).
\( \tilde{G} \) has identity and inverse obviously but not clearly associative.
Let’s define a map \( \tilde{G} \to G \) sending equivalence class \([a]\) to the end-point of it’s representative.
This is well-defined: the end-point doesn’t depend on the choice.
This is obviously a homomorphism, and it’s clearly surjective.
It’s also injective, so we get an isomorphism. Done.
Using the method above, see how it reconstructs the groups $\mathbb{Z}$, $\mathbb{Z}^2$ and $\mathbb{Z}/n$. 
1. Using the method above, see how it reconstructs the groups $\mathbb{Z}$, $\mathbb{Z}^2$ and $\mathbb{Z}/n$.

2. Can any graph appear as a Cayley graph of a group?
Free groups

1. Using the method above, see how it reconstructs the groups $\mathbb{Z}$, $\mathbb{Z}^2$ and $\mathbb{Z}/n$.

2. Can any graph appear as a Cayley graph of a group?

3. Think about how to construct a group with no relations (say, generated by two elements).
Free groups

1. Using the method above, see how it reconstructs the groups $\mathbb{Z}$, $\mathbb{Z}^2$ and $\mathbb{Z}/n$.

2. Can any graph appear as a Cayley graph of a group?

3. Think about how to construct a group with no relations (say, generated by two elements).
Normal subgroups

Definition

Let $G$ be a group, and $H$ be a subgroup. The subgroup $H$ is called normal if for any $g \in G$ we have $gHg^{-1} = H$ (equality of sets!).

In other words, $H$ is normal if and only if all left cosets are the same as right cosets, $gH = Hg$. If $G$ is abelian, every subgroup is normal.

The subgroup of rotations in the group $D_4$ of symmetries of a square is normal.

The subgroup $A_n$ of even permutations is normal in $S_n$.  

Sasha Patotski (Cornell University)  
Cayley graphs. Normal subgroups  
December 21, 2015  
10 / 13
Normal subgroups

**Definition**

Let $G$ be a group, and $H$ be a subgroup. The subgroup $H$ is called **normal** if for any $g \in G$ we have $gHg^{-1} = H$ (equality of sets!).

- In other words, $H$ is normal if and only if all left cosets are the same as right cosets, $gH = Hg$. 
Definition

Let $G$ be a group, and $H$ be a subgroup. The subgroup $H$ is called normal if for any $g \in G$ we have $gHg^{-1} = H$ (equality of sets!).

- In other words, $H$ is normal if and only if all left cosets are the same as right cosets, $gH = Hg$.
- If $G$ is abelian, every subgroup is normal.
Normal subgroups

Definition
Let $G$ be a group, and $H$ be a subgroup. The subgroup $H$ is called normal if for any $g \in G$ we have $gHg^{-1} = H$ (equality of sets!).

- In other words, $H$ is normal if and only if all left cosets are the same as right cosets, $gH = Hg$.
- If $G$ is abelian, every subgroup is normal.
- The subgroup of rotations in the group $D_4$ of symmetries of a square is normal.
Normal subgroups

Definition

Let $G$ be a group, and $H$ be a subgroup. The subgroup $H$ is called normal if for any $g \in G$ we have $gHg^{-1} = H$ (equality of sets!).

- In other words, $H$ is normal if and only if all left cosets are the same as right cosets, $gH = Hg$.
- If $G$ is abelian, every subgroup is normal.
- The subgroup of rotations in the group $D_4$ of symmetries of a square is normal.
- The subgroup $A_n$ of even permutations is normal in $S_n$. 
The point is: if $H$ is normal, the set of cosets $G/H$ has a natural group structure. This group is called the \textbf{quotient group}.

- We define $aH \ast bH := abH$. Prove that it’s well defined!
The point is: if $H$ is normal, the set of cosets $G/H$ has a natural group structure. This group is called the quotient group.

- We define $aH \ast bH := abH$. Prove that it’s well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\ldots, -n, 0, n, 2n, \ldots \}$. Prove that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.
The point is: if $H$ is normal, the set of cosets $G/H$ has a natural group structure. This group is called the quotient group.

- We define $aH \ast bH := abH$. Prove that it’s well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\ldots, -n, 0, n, 2n, \ldots \}$. Prove that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.
- Prove that $S_n/A_n \simeq \mathbb{Z}/2$. 

$\mathbb{R}/\mathbb{Z}$ is a circle $\mathbb{S}^1$. 

Sasha Patotski (Cornell University)  
Cayley graphs. Normal subgroups  
December 21, 2015 11 / 13
Cosets for normal subgroups

The point is: if $H$ is normal, the set of cosets $G/H$ has a natural group structure. This group is called the quotient group.

- We define $aH \ast bH := abH$. Prove that it's well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\ldots, -n, 0, n, 2n, \ldots \}$. Prove that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.
- Prove that $S_n/A_n \simeq \mathbb{Z}/2$.
- Prove that $G \times H/H \simeq G$, where $H \subset G \times H$ is the subgroup $H = \{(e, h) \mid h \in H\}$. 

Sasha Patotski (Cornell University)
The point is: if $H$ is normal, the set of cosets $G/H$ has a natural group structure. This group is called the **quotient group**.

- We define $aH \ast bH := abH$. Prove that it’s well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\ldots, -n, 0, n, 2n, \ldots \}$. Prove that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n$.
- Prove that $S_n/A_n \cong \mathbb{Z}/2$.
- Prove that $G \times H/H \cong G$, where $H \subset G \times H$ is the subgroup $H = \{(e, h) \mid h \in H\}$.
- $\mathbb{R}/\mathbb{Z}$ is a circle $S^1$. 

Let $G$ be a group and $K$ be another group, on which $G$ acts by automorphisms, i.e. isomorphisms to itself.

In other words, for each $g \in G$ we have assigned an isomorphism $A_g : K \rightarrow K$, such that $A_e = id$ and $A_{gh} = A_g \circ A_h$. We write $g \cdot k$ (or $g.k$) for $A_g(k)$. 

Note that $K$ is a normal subgroup in $G \rtimes K$, and $G \rtimes K / K \cong G$.

If $G$ acts trivially on $K$, then $G \rtimes K \cong G \times K$. 

The group $D_{2n}$ of symmetries of the $n$-gon is $\mathbb{Z}/2 \rtimes \mathbb{Z}/n$, where the action of $\mathbb{Z}/2$ on $\mathbb{Z}/n$ is by $a \mapsto -a$. 

Sasha Patotski (Cornell University) 
Cayley graphs. Normal subgroups 
December 21, 2015 12 / 13
Semidirect product

- Let $G$ be a group and $K$ be another group, on which $G$ acts by **automorphisms**, i.e. isomorphisms to itself.
- In other words, for each $g \in G$ we have assigned an isomorphism $A_g : K \to K$, such that $A_e = id$ and $A_{gh} = A_g \circ A_h$. We write $g \cdot k$ (or $g.k$) for $A_g(k)$.
- We define $G \rtimes K$ to be the set $K \times G$ with the operation

$$(k_1, g_1) \ast (k_2, g_2) = (k_1 \ g_1 k_2, g_1 \cdot g_2)$$

Note that $K$ is a normal subgroup in $G \rtimes K$, and $G \rtimes K / K \cong G$.

If $G$ acts trivially on $K$, then $G \rtimes K \cong G \times K$.

The group $D_{2n}$ of symmetries of the $n$-gon is $\mathbb{Z}/2 \rtimes \mathbb{Z}/n$, where the action of $\mathbb{Z}/2$ on $\mathbb{Z}/n$ is by $a \mapsto -a$. 

Sasha Patotski (Cornell University)
Semidirect product

- Let $G$ be a group and $K$ be another group, on which $G$ acts by **automorphisms**, i.e. isomorphisms to itself.

- In other words, for each $g \in G$ we have assigned an isomorphism $A_g : K \to K$, such that $A_e = id$ and $A_{gh} = A_g \circ A_h$. We write $g \cdot k$ (or $g.k$) for $A_g(k)$.

- We define $G \rtimes K$ to be the set $K \times G$ with the operation

$$ (k_1, g_1) \ast (k_2, g_2) = (k_1 \cdot g_1 k_2, g_1 \cdot g_2) $$

- Note that $K$ is a normal subgroup in $G \rtimes K$, and $G \rtimes K/K \simeq G$.
Let $G$ be a group and $K$ be another group, on which $G$ acts by automorphisms, i.e. isomorphisms to itself.

In other words, for each $g \in G$ we have assigned an isomorphism $A_g : K \to K$, such that $A_e = id$ and $A_{gh} = A_g \circ A_h$. We write $g.k$ (or $g.k$) for $A_g(k)$.

We define $G \rtimes K$ to be the set $K \times G$ with the operation

$$(k_1, g_1) \ast (k_2, g_2) = (k_1 g_1 k_2, g_1 \cdot g_2)$$

Note that $K$ is a normal subgroup in $G \rtimes K$, and $G \rtimes K / K \simeq G$.

If $G$ acts trivially on $K$, then $G \rtimes K \simeq G \times K$. 

The group $D_{2n}$ of symmetries of the $n$-gon is $\mathbb{Z}_{/2} \rtimes \mathbb{Z}_{/n}$, where the action of $\mathbb{Z}_{/2}$ on $\mathbb{Z}_{/n}$ is by $a \mapsto -a$. 

Sasha Patotski (Cornell University)
Let $G$ be a group and $K$ be another group, on which $G$ acts by **automorphisms**, i.e. isomorphisms to itself.

In other words, for each $g \in G$ we have assigned an isomorphism $A_g : K \rightarrow K$, such that $A_e = id$ and $A_{gh} = A_g \circ A_h$.

We write $g.k$ (or $g.k$) for $A_g(k)$.

We define $G \ltimes K$ to be the set $K \times G$ with the operation

$$(k_1, g_1) \ast (k_2, g_2) = (k_1^{g_1} k_2, g_1 \cdot g_2)$$

Note that $K$ is a normal subgroup in $G \ltimes K$, and $G \ltimes K / K \cong G$.

If $G$ acts trivially on $K$, then $G \ltimes K \cong G \times K$.

The group $D_{2n}$ of symmetries of the $n$-gon is $\mathbb{Z}/2 \ltimes \mathbb{Z}/n$, where the action of $\mathbb{Z}/2$ on $\mathbb{Z}/n$ is by $a \mapsto -a$. 

Semidirect product

Theorem

Let $G$ be a group, and $H, K$ are two subgroups. Suppose that

- $H \cap K = \{e\}$;
- $G = KH$ as a set;
- $K$ is a normal subgroup of $G$.

Then $G \cong H \rtimes K$, where the action of $H$ on $K$ is given by conjugation $h \cdot k = hkh^{-1}$. 