Cayley graphs. Normal subgroups

Sasha Patotski

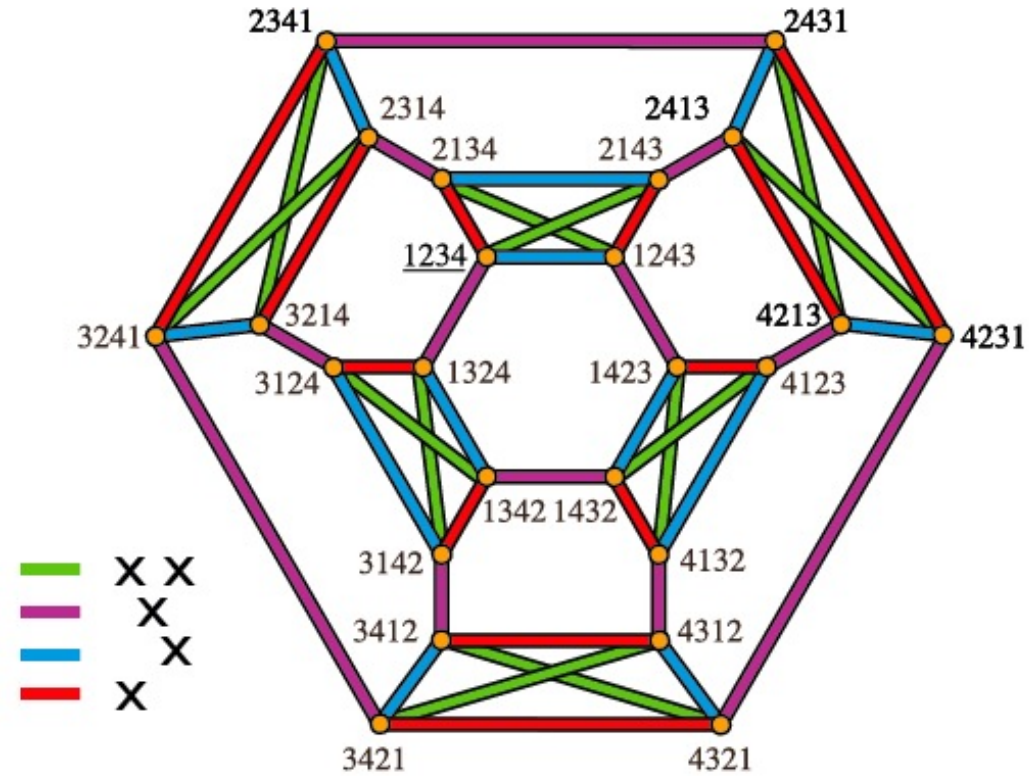
Cornell University

ap744@cornell.edu

December 21, 2015

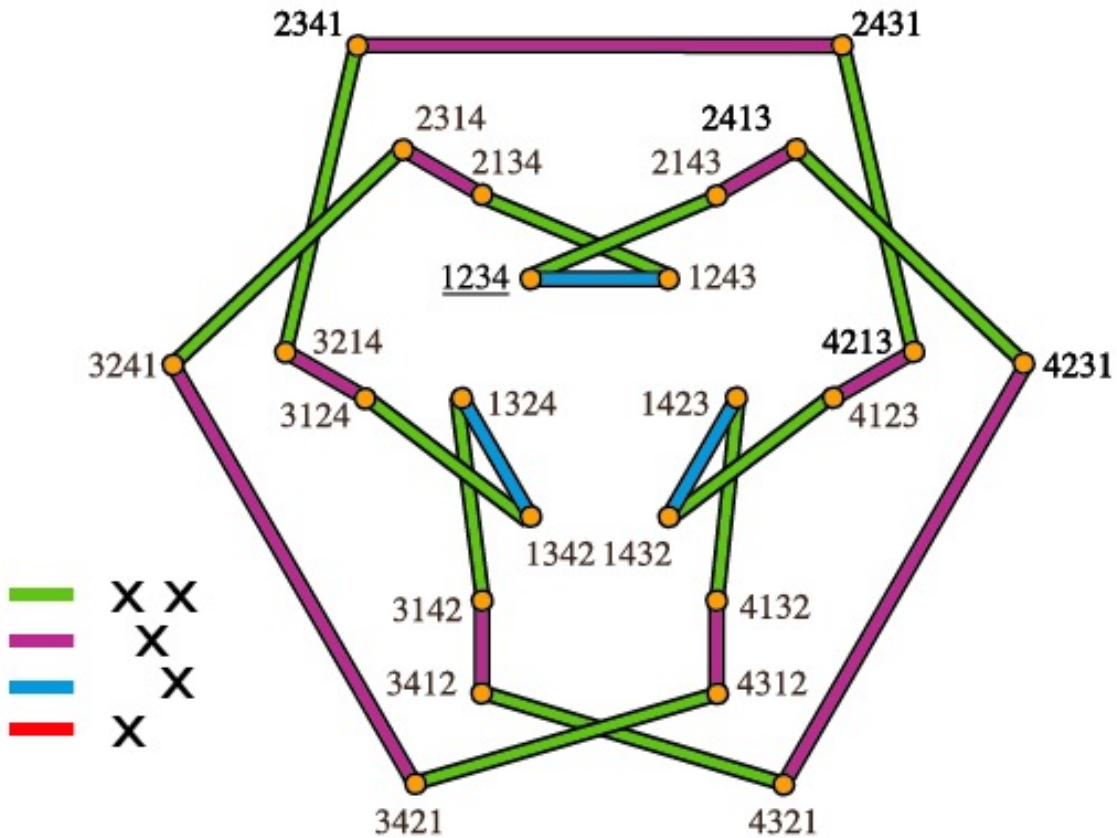
Graph out of bell ringing

- 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:



Cayley Graph

Let G be a group, and let S be a generating set of elements.

Definition

Let $Cay(G, S)$ 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 $S = \{1\}$.

Cayley Graph

Let G be a group, and let S be a generating set of elements.

Definition

Let $Cay(G, S)$ 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 $S = \{(1, 0), (0, 1)\}$?

Cayley Graph

Let G be a group, and let S be a generating set of elements.

Definition

Let $Cay(G, S)$ 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°) 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?

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?
- Any group acts on its Cayley graph, sending a vertex corresponding to h to the vertex corresponding to gh.

Group from its Cayley graph

1. Let $\Gamma = Cay(G, S)$ be a Cayley graph.
   Question (Mr. Drix): how to see group multiplication from it?

Group from its Cayley graph

1. Let $\Gamma = Cay(G, S)$ be a Cayley graph.
   Question (Mr. Drix): how to see group multiplication from it?

Group from its Cayley graph

1. Let $\Gamma = Cay(G, S)$ 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.

Group from its Cayley graph

1. Let $\Gamma = Cay(G, S)$ 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.
4. Let P_Γ be the set of paths in $\widetilde{\Gamma}$.

Group from its Cayley graph

1. Let $\Gamma = Cay(G, S)$ 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.
4. Let P_Γ be the set of paths in $\widetilde{\Gamma}$.
5. Let $\widetilde{G}$ be the set of equivalence classes of elements in P_Γ starting at the vertex e, where two paths are called equivalent iff they differ by (oriented) cycles.

Group from its Cayley graph

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

Group from its Cayley graph

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

Group from its Cayley graph

- Let $\widetilde{G}$ be the set of equivalence classes of paths in $\widetilde{\Gamma}$ starting at the vertex e, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let's define multiplication on $\widetilde{G}$. 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.

Group from its Cayley graph

- Let $\widetilde{G}$ be the set of equivalence classes of paths in $\widetilde{\Gamma}$ starting at the vertex e, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let's define multiplication on $\widetilde{G}$. 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 $e, s_{i_1}, s_{i_1}s_{i_2}, \ldots, s_{i_1}s_{i_2}\ldots s_{i_r} = h_0$.

Group from its Cayley graph

- Let $\widetilde{G}$ be the set of equivalence classes of paths in $\widetilde{\Gamma}$ starting at the vertex e, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let's define multiplication on $\widetilde{G}$. 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 $[a] * [b]$ 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 $g_0 h_0$.

Group from its Cayley graph

- Let $\widetilde{G}$ be the set of equivalence classes of paths in $\widetilde{\Gamma}$ starting at the vertex e, where two paths are called equivalent iff they differ by some (oriented) cycles.
- Let's define multiplication on $\widetilde{G}$. 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 $[a] * [b]$ 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:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.

Group from its Cayley graph

- **Claim:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.
- $\widetilde{G}$ has identity and inverse obviously but not clearly associative.

Group from its Cayley graph

- **Claim:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.
- $\widetilde{G}$ has identity and inverse obviously but not clearly associative.
- Let's define a map $\widetilde{G} \to G$ sending equivalence class $[a]$ to the end-point of it's representative.

Group from its Cayley graph

- **Claim:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.
- $\widetilde{G}$ has identity and inverse obviously but not clearly associative.
- Let's define a map $\widetilde{G} \to G$ 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.

Group from its Cayley graph

- **Claim:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.
- $\widetilde{G}$ has identity and inverse obviously but not clearly associative.
- Let's define a map $\widetilde{G} \to G$ 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.

Group from its Cayley graph

- **Claim:** $\widetilde{G}$ with the multiplication $*$ is a group, and is isomorphic to G.
- $\widetilde{G}$ has identity and inverse obviously but not clearly associative.
- Let's define a map $\widetilde{G} \to G$ 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.**

Free groups

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

Free groups

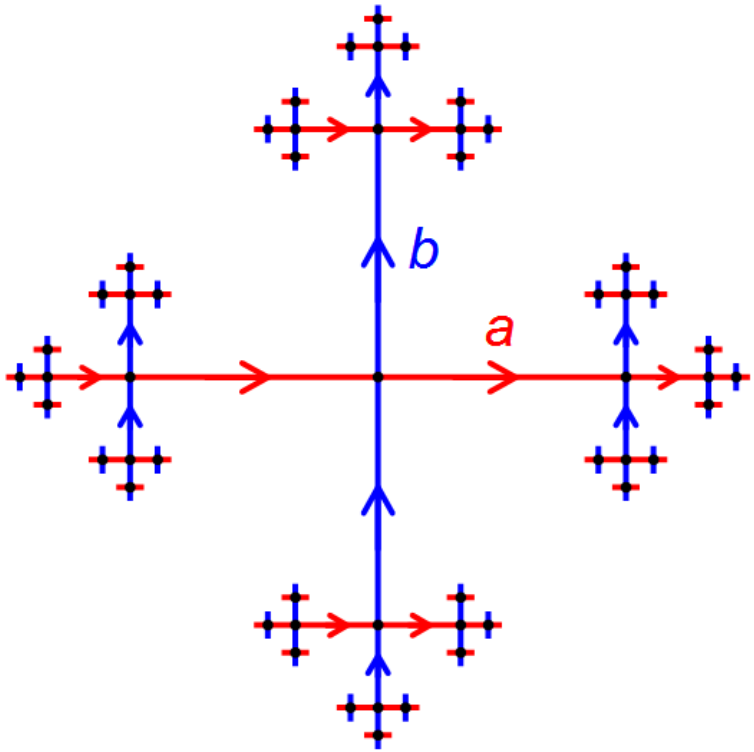
1. Using the method above, see how it reconstructs the groups $\mathbb{Z}$, $\mathbb{Z}^2$ and $\mathbb{Z}/n$.
2. Can any graph appear as a Cayley graph of a group?

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!).

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, $gH = Hg$.

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.

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.

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 $aH * bH := abH$. Prove that it's well defined!

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 $aH * bH := abH$. Prove that it's well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\dots, -n, 0, n, 2n, \dots\}$. Prove that $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.

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

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 $aH * bH := abH$. Prove that it's well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\dots, -n, 0, n, 2n, \dots\}$. 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 $H = \{(e, h) \mid h \in H\}$.

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 $aH * bH := abH$. Prove that it's well defined!
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\dots, -n, 0, n, 2n, \dots\}$. 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 $H = \{(e, h) \mid h \in H\}$.
- $\mathbb{R}/\mathbb{Z}$ is a circle S^1.

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 ${}^g k$ (or $g.k$) for $A_g(k)$.

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 ${}^g k$ (or $g.k$) for $A_g(k)$.
- We define $G \ltimes K$ to be the set $K \times G$ with the operation

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

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 ${}^g k$ (or $g.k$) for $A_g(k)$.
- We define $G \ltimes K$ to be the set $K \times G$ with the operation

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

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

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 ${}^g k$ (or $g.k$) for $A_g(k)$.
- We define $G \ltimes K$ to be the set $K \times G$ with the operation

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

- Note that K is a normal subgroup in $G \ltimes K$, and $G \ltimes K/K \simeq G$.
- If G acts trivially on K, then $G \ltimes K \simeq G \times K$.

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 ${}^g k$ (or $g.k$) for $A_g(k)$.
- We define $G \ltimes K$ to be the set $K \times G$ with the operation

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

- Note that K is a normal subgroup in $G \ltimes K$, and $G \ltimes K/K \simeq G$.
- If G acts trivially on K, then $G \ltimes K \simeq G \times K$.
- 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 $G \simeq H \ltimes K$, where the action of H on K is given by conjugation ${}^h k = hkh^{-1}$.