Simple groups. Jordan-Hölder theorem

Sasha Patotski

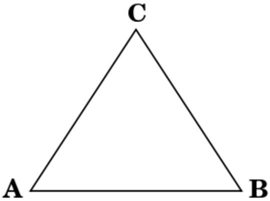
Cornell University

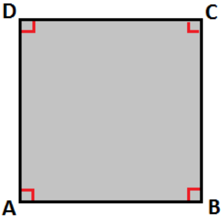
ap744@cornell.edu

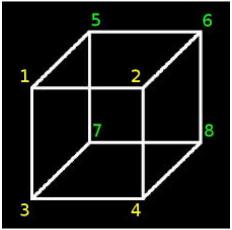
January 13, 2016

Symmetries of things give groups:

1. **triangle** $\rightsquigarrow S_3$;
2. **square** $\rightsquigarrow D_4$;
3. **cube** $\rightsquigarrow S_4 \times \mathbb{Z}/2$







- symmetries $\rightsquigarrow$ groups of transformations;
- groups of transformations $\rightsquigarrow$ abstract groups;

- symmetries $\rightsquigarrow$ groups of transformations;
- groups of transformations $\rightsquigarrow$ abstract groups;
- abstract groups are related by **homomorphisms**;

- symmetries $\rightsquigarrow$ groups of transformations;
- groups of transformations $\rightsquigarrow$ abstract groups;
- abstract groups are related by **homomorphisms**;
- homomorphism φ gives new groups: $\ker\varphi$ and $\operatorname{Im}\varphi$.

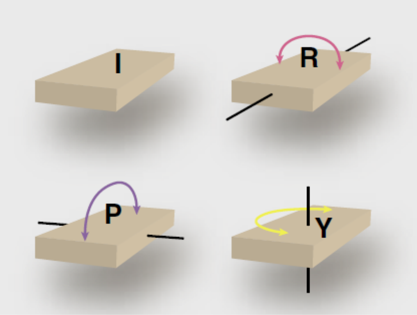
Group action

- Abstract groups can **act** on things. A group G acts on a set X via a homomorphism $G \to Bij(X)$.
- Action of a group – symmetries of the set.

Group action

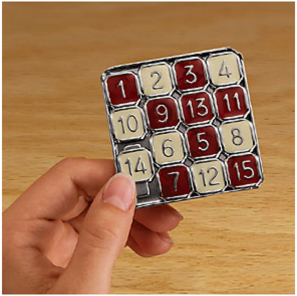
- Abstract groups can **act** on things. A group G acts on a set X via a homomorphism $G \to Bij(X)$.
- Action of a group – symmetries of the set.
- **Main point**: any abstract group is a group of symmetries of something, and vice versa.

Applications



There is no mattress flip, repeating which we can obtain all possible positions of a mattress.

Applications



Unsolvability of the "fifteen puzzle" with 14 and 15 flipped uses group theoretic invariants.

Applications

- $n!$ is divisible by $m!(n-m)!$ for $0 \le m \le n$;
- $(ab)!$ is divisible by $a!(b!)^a$;
- the number of integers mod n which are invertible mod n is an even number.

We can count number of necklaces (and many other things) using Polya Enumeration theorem.

Applications

Used labeling by elements of $\mathbb{Z}/2 \times \mathbb{Z}/2$ and symmetries of the "cross" to study possible game winning positions.

Applications

Bell ringing has a lot to do with subgroups of permutation groups, and paths Cayley graphs.

- What kind of groups can there possible exist?

Groups zoo

- What kind of groups can there possible exist?
- How does a "groups zoo" look like?

Sudoku group

The group of symmetries of a Sudoku game is

$$(\mathbb{Z}/2 \ltimes (S_3 \ltimes S_3^3)^2) \times S_9$$

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

The order of the groups above is $2 \cdot 6^8 \cdot 9! = 1,218,998,108,160$.

Can we classify all groups?

Can we classify all groups?

- **Answer:** NO WAY!

Can we classify all groups?

- **Answer:** NO WAY!
- **Question:** can we classify **finite** groups?

Can we classify all groups?

- **Answer:** NO WAY!
- **Question:** can we classify **finite** groups?
- **Answer:** SORT OF! (EXTREMELY HARD!)

Can we classify all groups?

- **Answer:** NO WAY!
- **Question:** can we classify **finite** groups?
- **Answer:** SORT OF! (EXTREMELY HARD!)
- **Question:** can we start with an easier problem, say classifying finite abelian groups?

Can we classify all groups?

- **Answer:** NO WAY!
- **Question:** can we classify **finite** groups?
- **Answer:** SORT OF! (EXTREMELY HARD!)
- **Question:** can we start with an easier problem, say classifying finite abelian groups?
- **Answer:** SURE! (FINITE) ABELIAN GROUPS ARE A PIECE OF CAKE!

Classification of finite abelian groups

Theorem

Any finite abelian group G is isomorphic to a product of cyclic groups with orders being powers of primes:

$$G \simeq \mathbb{Z}/p_1^{n_1} \times \mathbb{Z}/p_2^{n_2} \times \cdots \times \mathbb{Z}/p_r^{n_r}$$

Such a decomposition is unique if we require $n_i \geq 1$ and $p_1 \geq p_2 \geq \ldots \ldots p_r$.

Feeling

- **Remark:** $\mathbb{Z}/4 \neq \mathbb{Z}/2 \times \mathbb{Z}/2$.

Feeling

- **Remark:** $\mathbb{Z}/4 \neq \mathbb{Z}/2 \times \mathbb{Z}/2$.
- **Feeling:** abelian groups are like sand.

General finite groups

- **Question:** what about general groups?

General finite groups

- **Question:** what about general groups?
- **Answer:** they are build from simple pieces, which **we can actually classify!**
- **Goal:** explain what these “simple pieces” are, and what “built” really means.

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!).

- 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.

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!).

- 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.
- Important example: for any homomorphism $\varphi\colon G \to H$, $\ker\varphi$ is a **normal** subgroup of G.

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**.

- The multiplication of cosets is given by $aH * bH := abH$ (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**.

- The multiplication of cosets is given by $aH * bH := abH$ (well-defined!).
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\dots, -n, 0, n, 2n, \dots\}$. Then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.

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**.

- The multiplication of cosets is given by $aH * bH := abH$ (well-defined!).
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\ldots, -n, 0, n, 2n, \ldots\}$. Then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.
- **Point:** all normal subgroups of a group G are kernels of all possible homomorphisms $G \to H$.

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**.

- The multiplication of cosets is given by $aH * bH := abH$ (well-defined!).
- Let $n\mathbb{Z} \subset \mathbb{Z}$ be the subgroup $\{\dots, -n, 0, n, 2n, \dots\}$. Then $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n$.
- **Point:** all normal subgroups of a group G are kernels of all possible homomorphisms $G \to H$.
- **Key theorem:**

Theorem (The First Isomorphism theorem)

For any homomorphism $\varphi\colon G \to H$, there is a natural isomorphism

$$G/\ker\varphi \simeq \operatorname{Im}\varphi$$

Simple groups

Definition

A group G is called **simple** if it doesn't have non-trivial normal subgroups (i.e. except G and $\{e\}$).

- For a simple group G, any homomorphism $G \to H$ is either trivial, or injective.

Simple groups

Definition

A group G is called **simple** if it doesn't have non-trivial normal subgroups (i.e. except G and $\{e\}$).

- For a simple group G, any homomorphism $G \to H$ is either trivial, or injective.
- **Feeling:** a simple group is like a steel ball

- Simple groups will be our building blocks.

Examples of simple groups

- A group $\mathbb{Z}/n$ is simple if and only if n is a prime number.

Examples of simple groups

- A group $\mathbb{Z}/n$ is simple if and only if n is a prime number.
- We will see that there is a good analogy

$$\textbf{simple groups} \leftrightarrow \textbf{prime numbers}$$

Examples of simple groups

- A group $\mathbb{Z}/n$ is simple if and only if n is a prime number.
- We will see that there is a good analogy

  simple groups $\leftrightarrow$ **prime numbers**
- Symmetric groups S_n are never simple for $n \geq 3$, since they contain normal subgroups A_n.

Examples of simple groups

- A group $\mathbb{Z}/n$ is simple if and only if n is a prime number.
- We will see that there is a good analogy

simple groups $\leftrightarrow$ **prime numbers**

- Symmetric groups S_n are never simple for $n \geq 3$, since they contain normal subgroups A_n.
- The groups A_n are, however, simple for $n \geq 5$ (not trivial to prove!)
- We will see many more examples later.

Questions about simple groups

- **Questions:** what are the orders of simple groups? can any order appear? can there be several simple groups having the same order?

Questions about simple groups

- **Questions:** what are the orders of simple groups? can any order appear? can there be several simple groups having the same order?
- If a group has prime order p, then it's isomorphic to $\mathbb{Z}/p$.

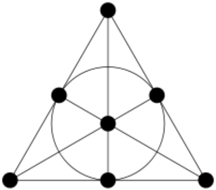
Questions about simple groups

- **Questions:** what are the orders of simple groups? can any order appear? can there be several simple groups having the same order?
- If a group has prime order p, then it's isomorphic to $\mathbb{Z}/p$.
- There are no simple groups of order 56.

Questions about simple groups

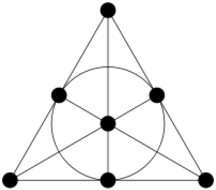
- **Questions:** what are the orders of simple groups? can any order appear? can there be several simple groups having the same order?
- If a group has prime order p, then it's isomorphic to $\mathbb{Z}/p$.
- There are no simple groups of order 56.
- There is **unique** simple group of order 168.

- **Theorem.** There is unique (up to isomorphism) simple group of order 168, which is the group of symmetries of the Fano plane:



Fano plane and the simple group of order 168

- **Theorem.** There is unique (up to isomorphism) simple group of order 168, which is the group of symmetries of the Fano plane:



- We will see how this example fits into a more general family of examples.

Crazy fact

- In fact, for any integer n there can be **at most two** groups of order n.

Crazy fact

- In fact, for any integer n there can be **at most two** groups of order n.
- For **almost all** integers n, there is at most **one** group of order n.

Crazy fact

- In fact, for any integer n there can be **at most two** groups of order n.
- For **almost all** integers n, there is at most **one** group of order n.
- There are two non-isomorphic simple groups of order 20160.
- There are two infinite families of groups, $O_{2n+1}(q)$ and $S_{2n}(q)$ (whatever they are), which have the same order for q odd and $n > 2$. **And that's it!**