

Given  $g_1, \dots, g_m \in S_n$ .

on board  
 Questions: How big is  $G := \langle g_1, \dots, g_m \rangle$ ?

2. Does  $\sigma \in G$ ?

3. If  $\sigma \in G$ , can you write it using  $g_1, \dots, g_m$ ?

4. Can you generate a strictly random  $\sigma \in G$ ?

"A group": 1. Associativity 2. Identity  
3. Inverses.

$S_n := \{ \text{all 1-1 onto } \sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \}$

1. Subgroups: "If  $S$  is finite and  $G \subset S$ , then

$G$  is a subgroup iff  $x, y \in G \Rightarrow xy \in G$ "

2. The Rubik's Cube group.

3. The group generated by  $g_1, \dots, g_m$

4. Complexity of brute force.

5. Gaussian elimination as on handout —  
simply write the algorithm and then explain.