Mathcamp Day 1

July-14-09
6:02 AM

Given $g_1 \ldots g_m \in S_n$.

on board:

Questions: 1. How big is $G := \langle g_1, \ldots g_m \rangle$?

2. Does $\sigma \in G$?

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

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

Today: 1. What do these questions mean?

2. How are they related to the Rubik cube?

3. Some preliminaries.

---

1. Define "a group". { easy claims: uniqueness of the identity & of inverses.
2. Examples $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{Z}/n$, $(\mathbb{Z}/p, \times)$, $S(X)$ and S_n, $GL(n)$, $\{\pm 1, \pm i, \pm j, \pm k\}$, Sym(object), and the most annoying choice of conventions in math ever.

   F_n (and $(ab)^{-1} = b^{-1}a^{-1}$)).
3. Abelian, Finite, order, for all of the above.
4. Subgroups: "If S is finite and $G \subset S$, then G is a subgroup iff $x, y \in G \Rightarrow xy \in G$"
5. The Rubiks Cube group.
6. The group generated by $g_1 \ldots g_m$
7. Complexity of brute force.

8. If time: every finite group is a subgroup of S_n, for some n [lovely but useless!].