TUTORIAL HOUR - 20/9

1 Orders of subgroups

You can run the code in `order.txt` on SAGE's online platform. The code lists all distinct orders of subgroups of a group G. Note that there can be more than one subgroup of the same cardinality.
Observe that S_3, D_3 and $\mathbb{Z}/6\mathbb{Z}$ have similar subgroups.
Do all their cayley tables match?

2 Equivalence relation

Let H be a subgroup of a group G.
Define a relation $\sim_H$ on the set G as $a \sim_H b$ if and only if $ab^{-1} \in H$.
Verify: This is an equivalence relation.

Use the symbol G/H to denote the set of equivalence classes $G/\sim_H$.
Let e be the identity element of G, then
Verify:
G/G has only one equivalence class.
Define a map $\phi : G \to G/\{e\}$ as $\phi(g) = [g]$, show that this is a bijection.

3 Assignment

This is not evaluative.

Suppose you'd like to communicate that you've understood the concept of subgroups without providing a proof.[1]

To test if you really did understand subgroups we'll consider $(\mathbb{Z}/2\mathbb{Z}, +, 0)$.
I'll pick up any subset of $\mathbb{Z}/2\mathbb{Z}$, even the empty set, and I'll ask if the picked subset is a subgroup. If you answer correctly, I'll continue to ask. If you answer incorrectly, I'll conclude that you haven't learnt anything about subgroups.

Maybe you don't know anything about subgroups and decide to randomly answer with YES or NO.
What is the probability that you'll randomly guess it right?

If I repeat this test a hundred times, what is the probability that you'll get all questions correct?

[1] A zero knowledge proof.

To make the test harder, the group on which you'll be tested on is a secret that will only be revealed at the test time.

Suppose you obtain information that you'll be tested using a group of order 4. The testing strategy was modified to a *two strikes you're out* policy, which means you are allowed to have one wrong answer.
Can you beat the 100 questions and skip learning the proof?
What would've of happened if the test wasn't lenient at all?

If you learn that the group is of order n, how many strikes would you need to beat the test and skip the proof?