TUTORIAL HOUR - 12/10

1 Required

1.1 Material

- Condensed notes on permutation groups from MATH 403, University of Maryland
- SageMath documentation for permutation groups

1.2 Exercises

1.2.1 Gallian

- Problems 1-7, 30-34, 40-45, Chapter 5, A First Course in Abstract Algebra

1.3 Programming

- Given a finite set of permutations in S_n, output the subgroup of S_n generated by these elements.
- Given a group G, perhaps one generated by the above set up, find all cyclic subgroups of G.
- Given any rational point P on the unit circle, which groups G_p does it belong to?
  Here G_p is the cyclic subgroup generated by $\left(\frac{a}{p}, \frac{b}{p}\right)$ where $a^2 + b^2 = p$ & $p \equiv 1 \pmod 4$.

2 Additional

2.1 Permutations and the Enigma machine

Interesting slides by Jiří Tůma about the allied effort to break the Enigma machine using permutation groups.

2.2 Two Groups One Claw

Consider a set-up consisting of two dials and a claw mechanism that can rotate both dials.
The claw mechanism accepts these instructions:

- `Move`: Moves the claw mechanism in front of the other dial.
- `Rotate`: Rotates the dial in front of the claw mechanism counterclockwise by 90 degrees.

Any finite combination of these instructions forms a plan (this includes the empty plan ϕ).

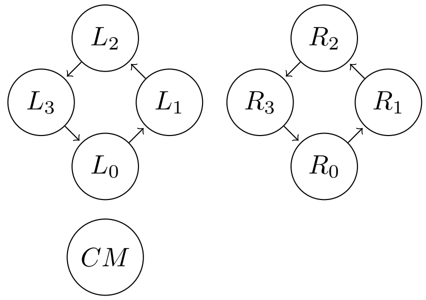

Figure 1: Initial State

2.2.1 Clawed Out

Define an equivalence relation on the set of all plans, $p_1 \sim_1 p_2$ if and only if they generate the same dial positions when executed separately from the initial state (it doesn't matter where the claw mechanism is).
Let X be the set of all equivalence classes formed by $\sim_1$ and $\star$ be the concatenation operator[1].

- Verify that the plan `move` is in the equivalence class $[\phi]$
- What is the cardinality of the group $(X, \star, [\phi])$
- How many subgroups does this group have?
- Using these two permutations
  - $(1, 2, 5, 11, 16, 15, 7, 3), (4, 9, 12, 8, 14, 6, 13, 10)$
  - $(1, 4)(2, 6)(3, 8)(5, 12)(7, 13)(9, 15)(10, 11)(14, 16)$

  generate the group G.
  Can you show that G and $(X, \star, [\phi])$ are isomorphic?

2.2.2 Dialled In

Define an equivalence relation on the set of all plans, $p_1 \sim_2 p_2$ if and only if they generate the same set-up when executed separately from the initial state (the position of the claw mechanism matters).
Let Y be the set of all equivalence classes formed by $\sim_2$.

- Is the plan `move` in the equivalence class of ϕ?
- What is the cardinality of the group $(Y, \star, [\phi])$?

[1] This behaves like the star operation described in the material provided on 27/8.

- Using these three permutations
  - $(1,9,17,25)(2,4,6,8)(3,11,19,27)(5,13,21,29)(7,15,23,31)(10,12,14,16)(18,20,22,24)(26,28,30,32)$
  - $(1,17)(2,6)(3,19)(4,8)(5,21)(7,23)(9,25)(10,14)(11,27)(12,16)(13,29)(15,31)(18,22)(20,24)(26,30)(28,32)$
  - $(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,20)(21,22)(23,24)(25,26)(27,28)(29,30)(31,32)$

  generate the group H.
  Can you show that H and $(Y, \star, [\phi])$ are isomorphic?