Homework #4

HW due Sunday 2/16 by pdf upload to Canvas; .tex source on the MATH 312 github repo.

General facts about subgroups

Problem 1 (the one-step subgroup test)**.** A subset $H \subseteq G$ is a subgroup if and only if the following condition holds:

$$\text{If } x, y \in H, \text{ then } xy^{-1} \in H. \tag{1}$$

Prove it! This will be super helpful for the rest of this assignment. Here's proof frames:

($\Rightarrow$) Suppose that $H \leq G$.
...
Therefore, whenever $x, y \in H$, $xy^{-1} \in H$.

($\Leftarrow$) Suppose that whenever $x, y \in H$, $xy^{-1} \in H$.
...
Therefore, $H \leq G$.

Problem 2. If $g \in G$, prove that $\langle g \rangle \leq G$. ("Cyclic subgroups are subgroups.")

Problem 3. Prove that $Z(G) \leq G$. ("The center of G is a subgroup of G.")

Problem 4. Consider the following (complete, correct) proof:

Theorem: If $S \subseteq G$, then $\langle S \rangle \leq G$.

Proof. Remember that $\langle S \rangle$ was defined as the set of "words in S", ie., finite products of finite powers of letters in S and their inverses:

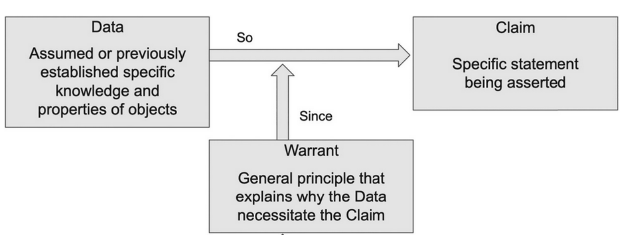
$$\langle S \rangle = \left\{ s_1^{p_1} \cdot s_2^{p_2} \cdot \ldots \cdot s_n^{p_n} \mid s_i \in S, p_i \in \mathbb{Z} \right\}.$$

Let $x = s_1^{p_1} \cdot s_2^{p_2} \cdot \ldots \cdot s_n^{p_n} \in \langle S \rangle$ and let $y = t_1^{q_1} \cdot t_2^{q_2} \cdot \ldots \cdot t_n^{q_n} \in \langle S \rangle$. By the shoes-and-socks theorem, $y^{-1} = t_n^{-q_n} \cdot \ldots \cdot t_2^{-q_2} \cdot t_1^{-q_1}$. Therefore,

$$\begin{aligned} xy^{-1} &= \left(s_1^{p_1} \cdot s_2^{p_2} \cdot \ldots \cdot s_n^{p_n} \right) \cdot \left(t_n^{-q_n} \cdot \ldots \cdot t_2^{-q_2} \cdot t_1^{-q_1} \right) \\ &= s_1^{p_1} \cdot s_2^{p_2} \cdot \ldots \cdot s_n^{p_n} \cdot t_n^{-q_n} \cdot \ldots \cdot t_2^{-q_2} \cdot t_1^{-q_1}. \end{aligned}$$

Since all the s_i's and all the t_i's are elements of S, and since all the p_i's and $-q_i$'s are integers, $xy^{-1} \in \langle S \rangle$. Therefore $\langle S \rangle \leq G$, thanks to Problem 1. □

Like the proof we saw in class that every subgroup of a cyclic group is cyclic, there are lots of things going on behind the scenes of this proof. See if you can break up this proof into data, claims, and (maybe implicit) warrants. (Click this small diagram for big.)



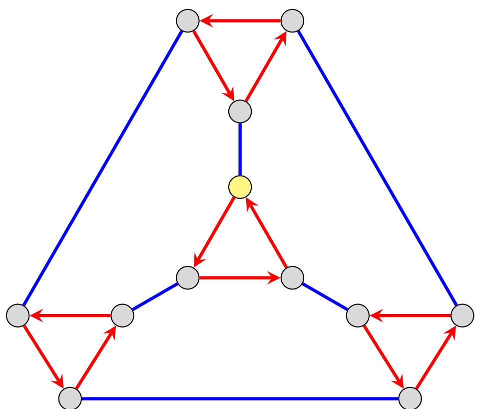
Helpful note: a warrant is a general principle and a data is a specific thing. For example, the group G that we're thinking about is a data, and the statement "group elements have inverses" is a warrant.

Subgroups of specific groups

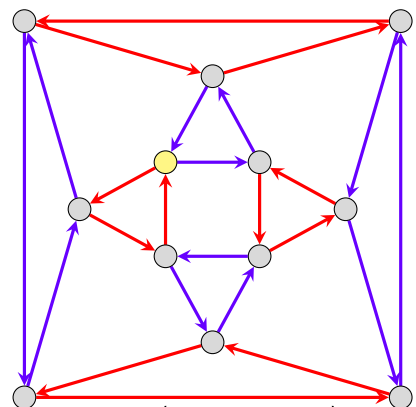
Problem 5. Construct the subgroup lattice for A_4. Remember, this is the set of all the even permutations in S_4, so it consists of the following 12 elements:

$$\begin{aligned}\text{0-cycles: } & () \\ \text{3-cycles: } & (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), \\ & (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3) \\ \text{Double transpositions: } & (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\end{aligned}$$

Here are two Cayley diagrams for A_4 with slightly different generating sets. I am including them in case they're helpful but mostly because I just think they're neat. The yellow node is the identity.



$A_4 = \langle (123), (12)(34) \rangle$



$A_4 = \langle (123), (234) \rangle$

Notes:

- Why are 3-cycles even permutations, you ask? Note that for instance $(1\ 2\ 3) = (1\ 2)(1\ 3)$.
- Please use the permutation calculator or this will take forever. Make sure left-to-right.
- Start by finding all the cyclic subgroups. Then "build up."
- I guarantee that all the subgroups will have order 1, 2, 3, 4, 6, or 12. (But I won't guarantee that there's subgroups of all those orders.)

Problem 6. This problem is about subgroups of an *infinite* group: the integers $(\mathbb{Z}, +)$. (Emphasis: we're writing this group *additively*, so it's like $a + b$ rather than ab, you know?).

(a) Show that the even integers, which we denote $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$, form a subgroup of $\mathbb{Z}$.

(b) Show that the odd integers are not a subgroup of $\mathbb{Z}$.

(c) Show that all subsets of the form $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$ are subgroups of $\mathbb{Z}$.

(d) Are there any other subgroups besides the ones listed in part (c)? Explain your answer.

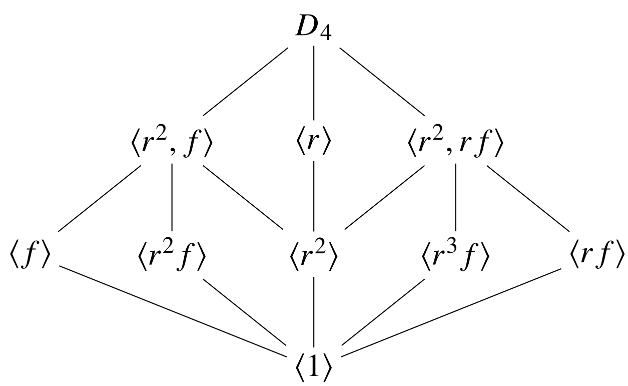
(e) For $n \in \mathbb{Z}$, write the subgroup $n\mathbb{Z}$ in the "generated by" notation. That is, find a set S such that $\langle S \rangle = n\mathbb{Z}$. (Maybe S is just one element.) Can you find more than one way to do it?

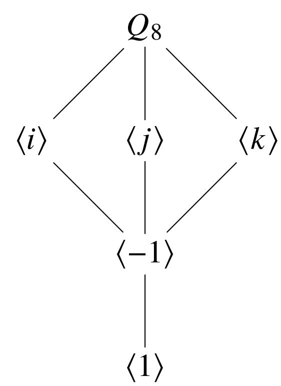
(f) Reflect on any different vibes in this infinite situation as opposed to the finite groups we've been working in so far. Did you have to adapt your strategies at all?

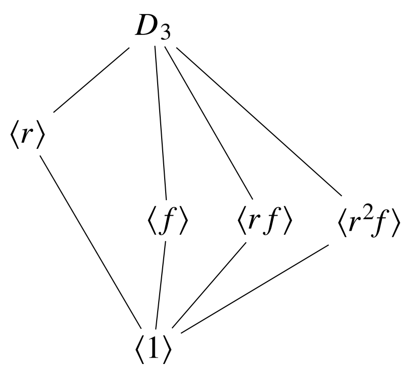
Centers of nonabelian groups

The center of an abelian group is boring: it is the whole group. The center of a non-abelian group is interesting: in some way, $Z(G)$ is a measurement of how non-abelian the group is. A cool thing about subgroup lattices is that they help us think about what $Z(G)$ is: since $Z(G) \leq G$, it must be one of the guys in the subgroup lattice.

Problem 7. Locate $Z(G)$ in the subgroup lattice of at least one, and maybe all, of these non-abelian groups. Refer to the slides, previous homeworks, and/or Group Explorer if you need reminders of how the operation works in each of these groups.



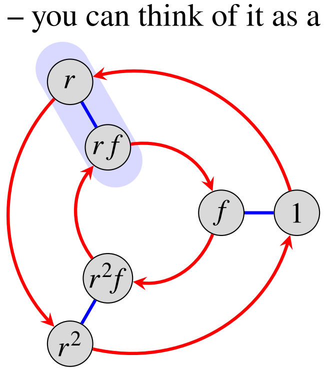




Challenge: A_4, whose lattice you drew in Problem 5.

Preview of next week: Cosets

When we looked for copies of C_2 inside of D_3, we noted this guy, who "has the same shape" as $C_2 \cong \langle f\rangle \leq D_3$ but isn't a subgroup because it doesn't include the identity. This guy is called a "coset" – you can think of it as a shifted version of a subgroup.



- Do you see any other cosets of $\langle f\rangle$?
- Can you find any cosets of $\langle rf\rangle$? (They're shaped a bit different, yeah?)
- How about $\langle r^2 f\rangle$?
- Can you find any cosets of $\langle r\rangle$?