Math 122: Algebra I, Fall 2023

Homework Assignment #8 (26 October 2023):
The action of G on itself by conjugation: class equation, $\mathrm{Aut}(G)$, etc.

> [...] lately our relation's not so well-defined
> And I just can't function without you
> I'll prove my proposition and I'm sure you'll find
> We're a finite simple group of order two
>
> —from *Finite Simple Group (of Order Two)* by The Klein Four, described by Lyrics Genius (https://genius.com/The-klein-four-finite-simple-group-of-order-two-lyrics) as "a very nerdy math song written and performed by a group of (at the time) graduate math students at Northwestern University."

This problem set is due Wednesday, ~~October 32~~ November 1 at midnight.

First, to complete the proof of Corollary 9 (if p is prime then every group of order p^2 is abelian), and the Example on pages 135–136:

1. [D&F 3.1, Exercise 36 (page 89)] Suppose G is a group such that the quotient group[1] $G/Z(G)$ is cyclic. Prove that G is abelian. [Choose some $x \in G$ such that the coset $xZ(G)$ generates $G/Z(G)$. Show that every $g \in G$ can be written as $x^a z$ for some $a \in \mathbf{Z}$ and $z \in Z(G)$, and check that any two such elements (possibly with different choices of a, z) commute.]

2. [Another route to the result of groups of order pq]
   i) For prime p and any group G, show that the number of order-p elements of G is $p - 1$ times the number of p-element subgroups of G.
   ii) Suppose G is a non-abelian group of order pq for distinct primes p, q. By the first problem, $Z(G)$ is trivial. Show that if $x \in G$ has order p then the conjugacy class of x has size q and vice versa. Use part (i) to deduce that if $p \not\equiv 1 \bmod q$ then the number of elements of order p in G is a multiple of $q(p-1)$, and vice versa. By Cauchy G does have elements of order p and elements of order q, so G must have at least $1 + q(p-1) + p(q-1)$ elements in all. Check that this must exceed pq, and deduce that one of p and q (necessarily the larger one) must be congruent to 1 modulo the other.

Conversely if one of p and q *is* congruent to 1 modulo the other then there does exist a non-abelian group of order pq; see the course website.

Some basics about conjugacy classes and the class equation:

3. [from D&F 4.3 Exercises 2–3] Find all conjugacy classes and the sizes in the following groups: i) A_4 ii) $S_3 \times S_3$ iii) $Z_3 \times A_4$

[1] We now know that in general $G/Z(G)$ is also the group of inner automorphisms of G.

4. [D&F 4.3 Exercise 13, extended] Prove that if a finite group G has at most 3 conjugacy classes then the conditions that $|G|$ be a multiple of $|Z(G)|$ and of each other term $|G : C_G(g_i)|$ of the class equation of G imply that this class equation is one of

$$|G| = 1, \quad |G| = 2, \quad |G| = 3, \quad |G| = 2 + 2, \quad |G| = 1 + 2 + 3.$$

Show that the fourth of these is impossible, while each of the others occurs for a unique group G. [In the last case, start from elements g, h of orders $2, 3$ respectively, and determine ghg^{-1}.]

In fact for each k there are only finitely many possible class equations for a finite group G with k conjugacy classes, and thus only finitely many possible G, though the list of all such G quickly becomes unmanageably huge.

5. [Rubik's Cube and group conjugation] The diagram below, repeated from Problem 4 of the second problem set (our first Rubik's Cube problem), shows the cubelets on two adjacent faces of Rubik's Cube:

1	**2**	**3**	3	4	5
6	**7**	**8**	8	9	10
11	**12**	**13**	13	14	15

Let s be the permutation of $\{1, 2, 3, \ldots, 15\}$ obtained by a 90° counterclockwise turn of the left face (columns 1–3), and let t be the permutation of $\{1, 2, 3, \ldots, 15\}$ obtained by a 90° counterclockwise turn of the right face (the other 3 columns). For example, $s(3) = 1$ and $t(3) = 13$. Also s^2 and t^2 are the 180° rotations σ, τ from that first Rubik's Cube problem.

i) In that first problem we showed that $(\sigma\tau)^3$, a.k.a. $s^2t^2s^2t^2s^2t^2$, acts by the double transposition (2 12) (4 14). Use this to determine the cycle structure of $st^2s^2t^2s^2t^2s$.

ii) How can we manipulate the Cube (no longer limiting ourselves to the s and t faces) to quickly obtain the double transposition (2 14) (8 10)?

Again you might want to check your answers with a physical or virtual Rubik's Cube. It is not too hard to adapt this construction to accomplish *any* double transposition of the edge cubelets; this provides a big part of one approach to solving the Cube: first place the corners, ignoring edges and possibly corner orientations; then use double transpositions to place the edges; finally fix any remaining corner rotations and edge flips.

Finally, a bit about normal and characteristic subgroups:

6. [D&F 4.4, Exercise 1] If σ is an automorphism of a group G, and $\varphi_g \in \mathrm{Aut}(G)$ is conjugation by g, prove that $\sigma \cdot \varphi_g \cdot \sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that the inner automorphisms of G form a normal subgroup of $\mathrm{Aut}(G)$. [The quotient group is called the "outer automorphism group" — somewhat misleadingly, because a non-identity element of this quotient group is not quite an outer automorphism but an *equivalence class* of outer automorphisms up to conjugation in G.]

7. [D&F 4.4, Exercises 6 and 8a] Let G be a group and K a subgroup of G.

i) Prove that if K is a characteristic subgroup of G then $K \lhd G$. Give an example of groups G and $K \lhd G$ such that K is not characteristic in G.

ii) Prove that if $K \lhd G$ and H is a characteristic subgroup of K then $H \lhd G$.