Homework Assignment 6

Due Friday, March 4

1. Let G be a group, and let A be a subset of G. Let's establish some facts about centralizers and normalizers.
   (a) Let A be a subset of G. Prove that $C_G(A) \leq G$.
   (b) Deduce the following chain of inclusions.
   $$Z(G) \leq C_G(A) \leq N_G(A) \leq G.$$
   (*Note:* In class we only defined the normalizer of a subgroup, but we can define the normalizer of a subset the same way: $N_G(A) = \{g \in G : gAg^{-1} = A\}$,)
   (c) Show that $C_G(A) = C_G(\langle A \rangle)$.
   (d) Give an example to show the analog of part (c) for normalizers is not true. That is, give $A \subseteq G$ where $N_G(A) \neq N_G(\langle A \rangle)$.
   (e) Show that if H is a subgroup of G, then $H \leq N_G(H)$.
   (f) Show that $H \leq C_G(H)$ if and only if H is abelian.

2. Compute the center of the dihedral group. Explicitly, let n be an integer ≥ 3. Compute $Z(D_{2n})$. (Note: you will need to split into the two cases, where n is even or n is odd).

3. In this exercise we see that we can learn important facts about groups by studying their quotients.
   (a) Suppose $H \leq Z(G)$. Show that H is a normal subgroup of G. (In particular, $Z(G)$ is normal).
   (b) Show that if $G/Z(G)$ is cyclic, then G is abelian.
   (c) Let p and q be prime numbers (not necessarily distinct), and G a group of order pq. Show that if G is not abelian, then $Z(G) = \{1\}$.

4. In this exercise we show that if G is a nonabelian group of order 6. We will show $G \cong S_3$.
   (a) Show that there is an element $x \in G$ of order 2. (Once we have Cauchy's theorem for nonabelian groups this part becomes easy, but since G has 6 elements, one can do this by inspection using Lagrange's theorem).
   (b) Let $x \in G$ have order 2, and let $H = \langle x \rangle$. Show that H is not normal in G. (*Hint:* Show that if H is normal then $H \leq Z(G)$, then apply 3(c) to find a contradiction.)
   (c) Define an action of G on the set $A = G/H$ by *left multiplication*: that is $g \cdot (xH) = gxH$. Show that this defines a well defined group action.
   (d) Consider the action of G on $A = G/H$ by left multiplication. Show that the associated permutation representation is injective. Conclude that $G \cong S_3$.

As we start defining more exotic properties of groups we will need to expand our library of finite groups to exhibit some of these interesting properties. We finish with two new examples of finite groups. First up: Quaternions.

Definition 1. *The quaternion group of order 8, denoted Q_8 is the group of the following 8 elements:*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

subject to the relations:

$$(-1)^2 = 1$$
$$i^2 = j^2 = k^2 = -1,$$
$$(-1)x = -x = x(-1) \text{ for all } x,$$

$$\begin{aligned} ij &= k, & ji &= -k, \\ jk &= i, & kj &= -i, \\ ki &= j, & ik &= -j. \end{aligned}$$

5. Let's establish some basic facts about Q_8. Much of this is worked out in the book.
   (a) Write the entire multiplication table for Q_8.
   (b) Find 2 elements which generate all of Q_8. (*Bonus:* Can you give a presentation of Q_8?)
   (c) Prove that Q_8 is not isomorphic to D_8.
   (d) Find all the subgroups of Q_8, and draw them in a lattice ordered by inclusion. (*Hint*: there are 6 total subgroups).
   (e) Prove that every subgroup of Q_8 is normal. (*Note*: we saw that if a group is abelian, every subgroup is normal. This shows the converse isn't true!)
   (f) Prove that every *proper* subgroup and quotient group of Q_8 is abelian (*Hint*: You can appeal to TH1#4).
   (g) Show that $Q_8/Z(Q_8)$ has order 4. By TH1 it must be isomorphic to Z_4 or V_4. Which one is it? Justify your answer. (*Hint for the second part*: you can do this by hand, but it might be slicker to apply 3(b)).

Let's finish by introducing finite matrix groups. We will need a definition.

Definition 2. *A field is a set F together with two commutative binary operations, $+$ and $\cdot$ (addition and multiplication), such that $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are abelian groups, and such that the distributive law holds. That is, for all $a, b, c \in F$ we have:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

For any field we let $F^\times = F \setminus \{0\}$ be its mutliplicative group. A field F is called a finite field if $|F| < \infty$.

It turns out that vector space theory over F is pretty much identical to vector space theory over R. We can define the first matrix group we hope to study.

Definition 3. *Let F be a field. If M, N are matrices with entries in F, we can compute their product MN and the determinant $\det(M) \in F$ using the same formulas as if $F = \mathbb{R}$. Then the general linear group of degree n over F is,*

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries in } F \text{ and } \det(A) \neq 0\}.$$

You may use the following fact without proof (since it is a standard result of linear algebra).

Proposition 1. *The set $GL_n(F)$ can be identified with the set of linear bijections $F^n \to F^n$, and matrix multiplication corresponds to composition of functions. In particular, $GL_n(F)$ is a group under matrix multiplication.*

6. It turns out that we have seen examples of finite fields already.
   (a) Let p be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ with the operations $+$ and $\times$ is a field. This is the *finite field of order* p and will be denoted by $\mathbb{F}_p$.
   (b) Show that if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field.
7. Now let's study $GL_2(\mathbb{F}_p)$.
   (a) Prove that $|GL_2(\mathbb{F}_2)| = 6$.
   (b) Write all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.
   (c) Show that $GL_2(\mathbb{F}_2)$ is not abelian. Conclude that it is isomorphic to S_3.
   (d) Generalizing part (a), show that if p is prime then
   $$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$