Takehome Assignment 1

Due Tuesday, February 22

In this assignment, we will prove an important result called *Lagrange's Theorem.* It goes as follows.

Theorem 1 (Lagrange's Theorem)**.**
If G is a finite group and H is a subgroup of G. Then:

(i) $|H|$ *divides* $|G|$.

(ii) $|G/H| = |G|/|H|$

(iii) $|H\backslash G| = |G|/|H|$.

We remind the you that $H\backslash G = \{Hx : x \in G\}$ is the set of *right cosets* of G. With this result in hand, we will be able to deduce a celebrated result of Fermat, which is central to number theory.

Theorem 2 (Fermat's Little Theorem)**.**
Let p be a prime number and a an integer. Then $a^p \equiv a \mod p$.

We will also be able to begin our mission of classifying finite groups up to isomorphisms, giving a complete answer for groups of order ≤ 5. To do all this, we will make the following definition.

Definition 1.
Let H be a group acting on a set A and fix $a \in A$. The orbit of a under H is the set

$$H \cdot a = \{b \in A \mid b = h \cdot a \text{ for some } h \in H\}.$$

Lets begin!

1. Let H be a group acting on a set A.
   (a) Show that the relation
   $$a \sim b \text{ if and only if } a = h \cdot b \text{ for some } h \in H$$
   is an equivalence relation on the set A.
   (b) Show that the equivalence classes of this equivalence relation are precisely the orbits of the elements of A under the action of H.
   (c) Conclude that the orbits of A under the action of H form a partition of A.

2. Let H be a subgroup of a group G, and let H act on G by left mulptilication.
   $$\begin{array}{rcl} H \times G & \to & G \\ (h, g) & \mapsto & hg \end{array}$$
   (a) Prove this is an action.
   (b) Fix $x \in G$, and consider its orbit $H \cdot x$. Show that H and $H \cdot x$ have the same cardinality. Deduce that all the orbits of G under the action of H have the same cardinality.
   (c) Now suppose further that G is a finite group. Use part (b) and exercise 1 to deduce the parts (i) and (iii) of Lagrange's theorem.
   (d) Observe that the argument we gave computed the number of right cosets. Modify your argument to deduce part (ii) of Lagrange's theorem.

3. We can use Lagrange's theorem and what we know about cyclic groups to prove Fermat's little theorem.
   (a) Let $|G| = n < \infty$. Fix some $x \in G$. Use Lagrange's theorem to show that $x^n = 1$.
   (b) Let p be a prime number. Compute the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. Fully justify your answer.
   (c) Combine parts (a) and (b) to prove Fermat's little theorem.
4. With Lagrange's theorem in hand, we can classify all finite groups of order ≤ 5.
   (a) We first classify all groups of prime order. Let $|G| = p$ for a prime number p. Show that G is cyclic. This take care of groups of order 2,3,5 (and infinitely more cases!). For today, only order 4 remains.
   (b) Suppose every element of G has order ≤ 2. Show that G is abelian.
   (c) Show that if $|G| = 4$, then G is abelian.
   (d) Prove that if $|G| = 4$, then $G \cong Z_4$ or $G \cong Z_2 \times Z_2$. (*Remark:* The latter of these two groups is called the *Klein 4-Group*, and is sometimes denoted V_4).
   (e) Explain why $Z_4 \ncong V_4$, thus showing our classification is not redundant.