Take Home Assignment 1

Due Monday, February 24

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 $|H|$ divides $|G|$.

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 $a^p \equiv a \mod p$.

To do all this, we will need 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.

   Proof. We must show $\sim$ is reflexive, symetric, and transitive. To see that $\sim$ is reflexive we use that $1 \in H$ acts trivially (since it is a group action). Therefore $a = 1 \cdot a$ so that $a \sim a$. To see that $\sim$ is symmetric, suppose $a \sim b$. Thus $a = h \cdot b$ for some $h \in H$. Therefore, we have:

   $$b = 1 \cdot b = (h^{-1}h) \cdot b = h^{-1} \cdot (h \cdot b) = h^{-1} \cdot (a)$$

   Thus $b \sim a$. Finally, if $a \sim b$ and $b \sim c$ we have $h, h' \in H$ with $a = h \cdot b$ and $b = h' \cdot c$. Thus

   $$a = h \cdot b = h \cdot (h' \cdot c) = hh' \cdot c,$$

   so that $a \sim c$ and $\sim$ is transitive. □

   (b) Show that the equivalence classes of this equivalence relation are precisely the orbits of the elements of A under the action of H.

   Proof. Fix $a \in A$. We compute the equivalence class $[a]$ of a.

   $$[a] = \{b : b \sim a\} = \{b : b = h \cdot a \text{ for some } h \in H\} = H \cdot a.$$

   Thus the equivalence class of a and the orbit of a agree. □

   (c) Conclude that the orbits of A under the action of H form a partition of A.

Proof. We showed (HW 1 Problem 4(a)) that the equivalence classes of an equivalence relation form a partition of a set. By part (b) the orbits of A under the action of H are the equivalence classes of the relation $\sim$ defined above, so they form a partition. $\square$

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) Fix $x \in G$, and consider its orbit $H \cdot x$. Show that H and $H \cdot x$ have the same cardinality. (Hint: build a bijective map $H \to H \cdot x$). Deduce that all the orbits of G under the action of H have the same cardinality.

Proof. We build a map $\varphi : H \to H \cdot x$ by the rule $\varphi(h) = hx$. This map by definition lands in $H \cdot x$, and has inverse $\varphi^{-1} : H \cdot x \to H$, given by the rule $\varphi^{-1}(g) = gx^{-1}$. We check that the image of φ^{-1} is in H. If $g \in H \cdot x$ then $g = hx$ some $h \in H$ so that

$$\varphi^{-1}(g) = gx^{-1} = hxx^{-1} = h \in H.$$

As the composition of φ and φ^{-1} is multiplication by $xx^{-1} = 1$ (or $x^{-1}x = 1$), they are inverses to eachother. Thus we have built a bijection betweeh H and $H \cdot x$ so they must have the same cardinality.

Now suppose we have two orbits $H \cdot x$ and $H \cdot y$. The argument above shows they both have cardinality equal to that of H, and therefore to eachother. $\square$

(b) Now suppose further that G is a finite group. Use part (a) and the exercise 1 to deduce Lagrange's theorem.

Proof. The orbits of the action of H on G form a partition of G. Since G is a finite group there are finitely many orbits. Let's list them: $\{H \cdot x_1, H \cdot x_2, \cdots, H \cdot x_r\}$, assuming that orbit appears exactly once. Since they form a partition of G, each element of G appears in exactly one orbit, so that:

$$|G| = |H \cdot x_1| + |H \cdot x_2| + \cdots + |H \cdot x_r|.$$

But by part (a), we have that $|H \cdot x_i| = |H|$ for each i. So we can conclude that $|G| = r|H|$, and so $|H|$ divides $|G|$. $\square$

.

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 $x^n = 1$.

Proof. Let $H = \langle x \rangle$. Then $|H| = |x|$, call it r. By Lagrange's theorem we have that $n = rk$ for some integer k. Thus $x^n = x^{rk} = (x^r)^k = 1^k = 1$. $\square$

(b) Let p be a prime number. Compute the order of $(\mathbb{Z}/p\mathbb{Z})^\times$. Fully justify your answer.

Proof. We know that $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/p\mathbb{Z} : \gcd(a,p) = 1\}$. But as p is prime, then for every $1 \leq a \leq p$, we have $\gcd(a,p) = 1$. Thus $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \cdots, \overline{p-1}\}$, and so $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ $\square$

(c) Combine parts (a) and (b) to prove Fermat's little theorem.

Proof. If $a \equiv 0 \mod p$ then $a^p \equiv 0 \mod p$ so the result certainly holds. Otherwise $\gcd(a,p) = 1$ and $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. By parts (a) and (b) we have $\overline{a}^{p-1} = 1$, so that

$$\overline{a}^p = \overline{a}^{p-1}\overline{a} = 1 \cdot \overline{a} = \overline{a},$$

and we win. $\square$