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

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

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 6(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. □

2. Let H be a subgroup of a group G, and let H act on G by left multiplication.

$$\begin{aligned} H \times G &\to G \\ (h, g) &\mapsto hg \end{aligned}$$

(a) Prove this is an action.

Proof. It is clear that $1 \cdot g = 1g = g$ so that the identity acts trivially. Futhermore, given $h, h' \in H$, we know by associativity of multiplication that

$$(hh') \cdot g = (hh')g = h(h'g) = h \cdot (h' \cdot g).$$

Therefore left multiplication is indeed 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.

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. □

(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.

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:

$$|G| = |H \cdot x_1| + |H \cdot x_2| + \cdots + |H \cdot x_r|. \tag{1}$$

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

$$|G| = r|H|, \tag{2}$$

and so $|H|$ divides $|G|$, proving part (i) of Lagrange's theorem. To deduce part (iii), we observe that the orbits $H \cdot x_i$ are precisely the right cosets Hx_i. In particular, the set

$$\{H \cdot x_1, H \cdot x_2, \cdots, H \cdot x_r\} = H\backslash G. \tag{3}$$

Thus $|H\backslash G| = r = |G|/|H|$ as desired. □

(d) Observe that the argument we gave computed the number of right cosets. Modify your argument to deduce part (ii) of Lagrange's theorem.

Proof. The crucial peices to prove part (iii) were that the right cosets formed a partition of G (by 2(a) and 1(c)), consisting of sets of size $|H|$ (by 2(b)). This immediately gives Equations 1,2 and 3 thereby giving the result. Therefore we must establish these two conditions for G/H. Let's spell it out carefully.

Let $G/H = \{x_1H, \cdots, x_sH\}$. We saw in class that these precisely the equivalence classes of *congruence modulo* H, (or if you like, these are the orbits of the action of H on G by right multiplication) so they form a partition of G. This immediately gives the analog to Equation 1:

$$|G| = |x_1H| + \cdots + |x_sH|.$$

To show they all have the same size, we can argue as in 2(b) above, that:

$$\begin{aligned} H &\longrightarrow xH \\ h &\mapsto xh \end{aligned}$$

is bijective, with inverse $h' \mapsto x^{-1}h'$. Therefore:

$$|G| = s|H| = |G/H||H|,$$

as desired. □

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 $x^n = x^{rk} = (x^r)^k = 1^k = 1$. □

(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 $1 \leq a < p$, 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 $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$ □

(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. □

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.

Proof. Fix an element $x \in G$ with $x \neq 1$, and consider $H = \langle x \rangle$. By Lagrange's theorem, $|H|$ divides p, so is either p or 1. Since $x \neq 1$, we know that $|H| \neq 1$, so that $|H| = p$. This implies $H = G$, and so x generates all of G. This is the definition of G being cyclic. □

(b) Suppose every element of G has order ≤ 2. Show that G is abelian.

Proof. Let $x, y \in G$. In any group there is some c such that $xy = cyx$. Indeed, solving for c gives

$$c = xyx^{-1}y^{-1}.$$

We hope to compute that $c = 1$. As x and y both have order ≤ 2, we have $x^{-1} = x$ and $y^{-1} = y$. Thus:

$$c = xyx^{-1}y^{-1} = xyxy = (xy)(xy) = 1,$$

as $|xy| \leq 2$ as well.

Remark. *In general the element $c = xyx^{-1}y^{-1}$ is called the commutator of x and y and is often denoted $[x, y]$. It measures how well x and y commute. It will be studied in more detail in Homework 7.*

□

(c) Show that if $|G| = 4$, then G is abelian.

Proof. If G has an element x of order 4 then $G = \langle x \rangle \cong Z_4$ is cyclic, and therefore abelian. Otherwise, every element of G has order < 4, but the order of every element must at least divide 4 so every element of G has order ≤ 2. Thus by part (b) G must be 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).

Proof. If G is not Z_4 then $G = \{1, a, b, c\}$ with $|a| = |b| = |c| = 2$. Let's compute ab. If $ab = a$ then $b = 1$, so this cannot happen. Similarly, $ab \neq b$, and as $a^{-1} = a \neq b$, we also have $ab \neq 1$. Thus $ab = c$. As G is abelian by part (b) we have $ba = c$ as well. And from here we derive that $ac = b$ and $bc = a$ using that every element is its own inverse. One can now observe by inspection that this produces precisely the multiplication table for

$Z_2 \times Z_2$. More explicitly Let $Z_2 \times Z_2 = \{(1,1),(x,1),(1,y),(x,y)\}$ with mutliplication done componentwise and $x^2 = y^2 = 1$. Define a map $\varphi : Z_2 \times Z_2 \to G$, by the rule:

$$(1,1) \mapsto 1,$$

$$(x,1) \mapsto a,$$

$$(1,y) \mapsto b,$$

$$(x,y) \mapsto c.$$

Then φ is bijective. We check:

$$\varphi(x,1)\varphi(1,y) = ab = c = \varphi(x,y),$$

$$\varphi(x,1)\varphi(x,y) = ac = b = \varphi(1,y),$$

$$\varphi(1,y)\varphi(x,y) = bc = a = \varphi(x,1),$$

so that φ is a homomorphism, thus an isomorphism. □

(e) Explain why $Z_4 \ncong V_4$, thus showing our classification is not redundant.

Proof. By Homework 3 Problem 1(e) an isomorphism between Z_4 and V_4 would have to take the generator of Z_4 to an element of order 4 in V_4, but V_4 has no elements of order 4. □