Mathematics 546 Homework.

We start with some problems related to subgroups.

Definition 1. Let G be a group. Then the ***center*** of G, denoted by $Z(G)$, is the set of elements of G that commute with all the elements of G. That is

$$Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}.$$

Problem 1. Show that $Z(G)$ is a subgroup of G. $\square$

Recall that the dihedral group D_n is the group generated by two elements a and b with

$$a^n = b^2 = 1, \quad ba = a^{-1}b.$$

Here (again) is the multiplication table for the quaternion group Q:

	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Problem 2. (a) Show that the center of the dihedral D_3 is trivial, that is $Z(D_3)$ is just the one element subgroup $\{1\}$.
(b) Show center of the dihedral group D_4 is $Z(D_4) = \{1, a^2\}$.
(c) Find the center of Q. $\square$

Definition 2. Let G be a group and $a \in G$. Then the ***centralizer*** of a, denoted $C(a)$, is the set of all element of G that commute with a. That is

$$C(a) = \{x \in G : ax = za\}.$$

$\square$

Problem 3. (a) In D_4 find $C(a)$ and $C(b)$.
(b) In Q find $C(i)$.
(c) In $\mathrm{GL}(2, \mathbb{R})$ (the group of invertible 2×2 matrices) find $C(A)$ where $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\square$

If G is a group and $a \in G$ then a has ***finite order*** if and only if there is a positive integers k with $a^k = e$ (where e is the identity of G). The ***order***, denoted $o(a)$ of a is then the smallest positive integer n with $a^n = 1$.

Proposition 3. *If a is a group element with finite order and $a^k = e$, then $o(a) \mid k$.*

Proof. We proved this in class: here is a recap of the argument. Let $n = o(a)$. Then n is the smallest positive integer with $a^n = e$. Use the division algorithm to divide n into k:

$$k = qn + r \qquad \text{with} \qquad 0 \le r < n.$$

Then

$$e = a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r.$$

Since $0 \le r < n$ and n is the smallest positive integer with $a^n = e$ this implies $r = 0$. But then $k = qn + r = qn$ which implies $k \mid n$. $\square$

We have also defined the ***cyclic subgroup*** generated a as

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

In class we proved

Proposition 4. *If a has finite order then $|\langle a \rangle| = o(a)$. (Here $|S|$ is the number of elements in the set S.)* $\square$

Problem 4. Let $a \in G$ have $o(a) = n$ and assume that $\gcd(k, n) = 1$. Show that $o(a^k) = o(a) = n$. *Hint:* First note

$$(a^k)^n = (a^n)^k = e^k = e$$

and $o(a^k)$ is the smallest positive integers m with $(a^k)^m = e$ thus $o(a^k) \le n$. Let $m = o(a^k)$. Then $(a^k)^m = a^{km} = e$ and by Proposition 3 this implies $n \mid km$. Now use that $\gcd(n, k) = 1$ to explain why $n \mid m$ and use this to finish the proof. $\square$

Let G be a group a H a subgroup of G. Then the ***right cosets*** of H are the sets

$$Hg = \{hg : h \in H\}$$

where $g \in G$.

Problem 5. (a) In D_3 list all the cosets of $H = \langle a \rangle = \{1, a, a^2\}$ (there are two of them).
(b) In D_4 list all the cosets of $H = \langle a^2 \rangle = \{1, a^2\}$ (there are four of them).
(c) In D_4 list all the cosets of $H = \{1, ab\} = \langle ab \rangle$ (there are four of them).
(d) In Q list all the cosets of $\langle k \rangle = \{1, k, -1, -k\}$ (there are two of them).

We have proven the following in class:

Proposition 5. *Let G be a group and H a subgroup of G. The for any $g \in G$ the there is a bijective function $f \colon H \to H_g$. Therefore if H is finite every coset of H has the same number of elements as H. (In symbols $|Hg| = |H|$.)*

Problem 6. Prove this. *Hint:* While we did this in class, it is worth repeating as the ideas are important. Recalling that $Hg = \{hg : h \in H\}$ it is natural to define $f\colon H \to Hg$ by

$$f(h) = hg.$$

If $h \in H$, then $f(h) = hg \in Hg$. So f maps H into the coset Hg.

(a) Show that f is injective (i.e. one-to-one). That is show if $f(h_1) = f(h_2)$, then $h_1 = h_2$.
(b) Show f is surjective (i.e. onto). That is show that for all $y \in Hg$ that there is a $h \in H$ with $f(h) = y$. (Do not make this hard. If $y \in Hg$, then by definition of Hg where is an $h \in H$ such that $y = hg$ and which point you are 96.32% of the way done in showing f is surjective.) □

The following is really just a corollary of Proposition 5 but is important enough to be called a theorem.

Theorem 6. *Let H be a finite subgroup of the group G. Then every two cosets of H have the same number of elements.*

Proof. Let Hg_1 and Hg_2 be cosets of H. Then

$$|Hg_1| = |H| = |Hg_2|.$$

as required. □

Proposition 7. *If H is a subgroup of the group G and Hg_1 and Hg_2 cosets of H. Then Hg_1 and hg_2 are either equal or disjoint. That is exactly one of the following hold:*

(i) $Hg_1 = Hg_2$, *or*
(ii) $Hg_1 \cap Hg_2 = \varnothing$.

Problem 7. Prove this. *Hint:* If $Hg_1 \cap Hg_2 = \varnothing$, then we are done so it is enough to show that

$$Hg_1 \cap Hg_2 \neq \varnothing \quad \text{implies} \quad Hg_1 = Hg_2.$$

To get started note that as $Hg_1 \cap Hg_2 \neq \varnothing$ there is at an element $x_0 \in Hg_1 \cap Hg_2$. By the definitions of Hg_1 and Hg_2 this implies there are $h_1, h_2 \in H$ with

$$x_0 = h_1 g_1 = h_2 g_2.$$

(a) Show
$$g_1 = (h_1^{-1}h_2)g_2 \quad \text{and} \quad g_2 = (h_2^{-1}h_1)g_1.$$
(b) Let $x \in Hg_1$. Then $x = hg_1$ for some $h \in H$. Use a formula from part (a) to get
$$x = hg_1 = h\left((h_1^{-1}h_2)g_2\right) = (hh_1^{-1}h_2)g_2$$
and explain why this implies $x \in Hg_2$. Thus $x \in Hg_1$ implies $x \in Hg_2$, that is $Hg_1 \subseteq Hg_2$.
(c) Do a similar argument to show $Hg_2 \subseteq Hg_1$.
(d) Put the pieces together to conclude $Hg_1 = Hg_2$. □

The following is a basic counting principle. Let S be a finite set and assume that S can be written as a disjoint union of some of its subsets:

$$S = S_1 \cup S_2 \cup \cdots \cup S_k,$$

where $S_1 \cap S_j = \varnothing$ when $i \neq j$. Then the number of elements in S is

$$|S| = |S_1| + |S_2| + \cdots + |S_k|.$$

Somewhat informally, if we have k bowls that the j-th bowl has m_j apples in it, then the total number of apples in the bowls is

$$n = m_1 + m_2 + \cdots + m_k.$$

In the case where each bowl as the same number of apples, say $m_j = m$ for all j then the total number of apples is

$$n = km.$$

Theorem 8. *(Lagrange's Theorem) Let G be a finite group and H a subgroup of G. Let k be the number of right cosets of H in G. Then*

$$|G| = k|H|.$$

Therefore $|H| \mid |G|$, and thus the order of any subgroup of G divides the order of G.

Problem 8. Show you are as cleaver as Lagrange by giving a proof of Theorem 8. *Hint:* If you want a start in the right direction let Hg_1, Hg_2 ,..., Hg_k be the k cosets of H. Then by Proposition 7 $Hg_i \cap Hg_j = \varnothing$ for $i \neq j$. Also

$$G = Hg_1 \cup Hg_2 \cup \cdots \cup Hg_k,$$

and by Proposition 6 we have $|Hg_j| = |H|$ for all j. Now think about counting apples in bowls. $\square$