PRINT Your Name:______________________________

There are 7 problems on 5 pages. Problems 1 and 2 are worth 10 points each. Each of the other problems is worth 6 points.

If I know your e-mail address, I will e-mail your grade to you. If I don't already know your e-mail address and you want me to know it, then **send me an e-mail**.

If you would like, I will leave your exam outside my office after I have graded it. (If you like, I will send you an e-mail when I am finished with it.) You may pick it up any time between then and the next class. **Let me know if you are interested.**

I will post the solutions on my website tonight after the exam is finished.

1. **STATE and PROVE Lagrange's Theorem.**

Lagrange's Theorem. *If H is a subgroup of the finite group G, then the order of H divides the order of G.*

Proof. We show

(a) Every element of G is in some left coset of H in G.

(b) If two left cosets of H in G have any element in common, then these two cosets are equal.

(c) Every left coset of H in G has the same number of elements as H.

Once we have established (a), (b), and (c), then we will have partitioned G into a handful of disjoint subsets and each of the subsets has the same number of elements as H. In other words, we will know that $|G| = r|H|$, where we use $|S|$ to represent the number of elements in the set S and r is the number of left cosets of H in G.

The proof of (a): If g is an element of G, then g is in the left coset gH.

The proof of (b): Suppose a and b are elements of G and x is an element of both cosets aH and bH. Thus, $x = ah_1$ and $x = bh_2$ for some h_1 and h_2 in H. It follows that $ah_1 = bh_2$; that is, $a = bh_2h_1^{-1}$. But H is a group so, $h_2h_1^{-1}$ is an element of H; let this element be called h_3. We have $\boxed{a = bh_3}$. We now prove that $aH = bH$.

$\subseteq$: Take an arbitrary element ah from aH, for some h in H. We see that $ah = bh_3h$, which is in bH because H is a group.

$\supseteq$: Take an arbitrary element bh' from bH, for some h' in H. We see that $bh' = ah_3^{-1}h$, which is in aH because H is a group.

The proof of (c): We exhibit a one-to-one correspondence between H and the coset aH for any fixed a in G. Define the function $\varphi\colon H \to aH$ by $\varphi(h) = ah$ for each h in H. Notice that every element of aH is in the image of φ. (Indeed, a typical element of aH has the form ah for some h in H, and this element is equal to $\varphi(h)$.) Notice that φ is one-to-one. (Indeed, if h_1 and h_2 are elements of H with $\varphi(h_1) = \varphi(h_2)$, then $ah_1 = ah_2$. Multiply by a^{-1} to see that $h_1 = h_2$.)

We have established (a), (b), and (c); therefore, we have completed the proof. $\square$

2. **Let G be a group and g be an element of G.**
   (a) Define the *center*, $Z(G)$, of G.
   (b) Define the *centralizer*, $C_G(g)$, of g in G.
   (c) Is it always true that $C_G(g) \subseteq Z(G)$? If yes, prove it. If no, give a counterexample.
   (d) Is it always true that $Z(G) \subseteq C_G(g)$? If yes, prove it. If no, give a counterexample.

   (a) The *center* of the group G is the set of all elements in G which commute with every element in G.
   (b) The *centralizer* of the element g in the group G is the set of all elements in G which commute with g.
   (c) No. Consider the group $G = D_3$ and the element $g = \sigma$ of G. In this case, $C_g(G) \not\subseteq Z(G)$. Indeed, the center of D_3 is $\{\text{id}\}$ because,

   $$\sigma\rho \neq \rho\sigma \tag{1}$$

   since the right side is $\sigma\rho^2$;

   $$\sigma\rho^2 \neq \rho^2\sigma \tag{2}$$

   since the right side is $\sigma\rho$;

   $$\sigma(\sigma\rho) \neq (\sigma\rho)\sigma \tag{3}$$

   since the left side is ρ and the right side is ρ^2; and

   $$\sigma(\sigma\rho^2) \neq (\sigma\rho^2)\sigma \tag{4}$$

   since the left side is ρ^2 and the right side is ρ. Line (1) tells us that $\sigma \notin Z(D_3)$ and $\rho \notin Z(D_3)$. Line (2) tells us that $\rho^2 \notin Z(D_3)$. Line (3) tells us that $\sigma\rho \notin Z(D_3)$. Line (4) tells us that $\sigma\rho^2 \notin Z(D_3)$. On the other hand, $\sigma \in C_G(g)$ because σ commutes with $g = \sigma$.
   (d) Yes. It is always true that $Z(G) \subseteq C_G(g)$. If x is in $Z(G)$, then x commutes with every element of G; hence, x commutes with the element g of G and $x \in C_G(g)$.

3. **(Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let H and K be subgroups of the group G with $H \neq \{\textbf{id}\}$ and $K \neq \{\textbf{id}\}$. Is it always true that $H \cap K \neq \{\textbf{id}\}$?**

No. Let G be the subgroup $\{\text{id}, \sigma, \rho^2, \sigma\rho^2\}$ of D_4; H be the subgroup $\{\text{id}, \sigma\}$ of G, and K be the subgroup $\{\text{id}, \rho^2\}$ of G. It is clear that $H \neq \{\text{id}\}$ and $K \neq \{\text{id}\}$. It is also clear that $H \cap K = \{\text{id}\}$.

4. **(Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let G be a group in which every proper subgroup is cyclic. Does the group G have to be cyclic?**

No. Let G be D_3. The proper subgroups of G have order 1, 2, or 3 by Lagrange's Theorem. The only subgroup of order 1 is $\{\text{id}\}$ and this group is cyclic. Every group of prime order is cyclic by the first application of Lagrange's Theorem. So, every proper subgroup of D_3 is cyclic, but D_3 is not cyclic.

5. **(Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let G be a group and let S be the subset $S = \{x \in G \mid x^2 = \mathbf{id}\}$ of G. Is S always a subgroup of G?**

No. Let G be D_3. The set S is equal to $\{\text{id}, \sigma, \sigma\rho, \sigma\rho\}$. Lagrange's Theorem tells us that S is not a subgroup of G because S has 4 elements, G has 6 elements and 4 does not divide into 6 evenly.

6. **(Yes or No. If yes, PROVE it. If no, give a COUNTEREXAMPLE.) Let G be an abelian group and let S be the subset**

$$S = \{x \in G \mid x^2 = \mathbf{id}\}$$

of G. Is S always a subgroup of G?

yes. The set S is **non-empty** because the identity element of the group G is in S. We establish **closure**. Take x and y from S. Observe that $(xy)^2 = xyxy = x^2y^2$ because G is abelian and $x^2y^2 = \text{id}$ because x and y are in S; and therefore, $xy \in S$. We establish the **inverse** axiom. Take $x \in S$. Let x^{-1} be the name of x's inverse in G. We must show that x^{-1} is also in S. We know $x^2 = id$. Multiply both side of the equation by $x^{-1}x^{-1}$ to see that $\text{id} = x^{-1}x^{-1}$; and therefore, $x^{-1} \in S$.

7. **List the left cosets of the subgroup $H = \{\mathbf{id}, \rho, \rho^2, \rho^3\}$ in the group $G = D_4$. I do not need to see many details.**

The left cosets of the subgroup $H = \{\text{id}, \rho, \rho^2, \rho^3\}$ in the group $G = D_4$ are

$$\text{id}H = \{\text{id}, \rho, \rho^2, \rho^3\} \quad \text{and} \quad \sigma H = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}.$$