Math 546, Exam 2, Spring, 2023

You should KEEP this piece of paper. Write everything on the **blank paper provided**. Return the problems **in order** (use as much paper as necessary), use **only one side** of each piece of paper. Number your pages and write your name on each page. Take a picture of your exam (for your records) just before you turn the exam in. I will e-mail your grade and my comments to you. I will keep your exam. **Fold your exam in half** before you turn it in.

No calculators, cell phones, computers, notes, etc.

Make your work correct, complete, and coherent.

The exam is worth 50 points.

The solutions will be posted later today.

(1) (8 points) **State and prove Lagrange's Theorem.**

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

Proof. Observe that every element of G is in exactly one left coset of H in G. Indeed, if $g \in G$, then g is in the coset gH. Furthermore, if two left cosets of H in G have any elements in common, then the two cosets are equal. Let $g \in aH \cap bH$ for some a, b, g in G. We prove $aH = bH$.

At any rate $g \in aH \cap bH$; so $g = ah_1$ and $g = bh_2$ for some h_1 and h_2 in H.

$\underline{aH \subseteq bH}$: Take an arbitrary element ah in aH (with $h \in H$). Observe that

$$ah = gh_1^{-1}h = bh_2h_1^{-1}h \in bH$$

because h_2, h_1^{-1}, and h are all in H and H is a group. Thus $aH \subseteq bH$.

$\underline{bH \subseteq aH}$: Take an arbitrary element bh' in aH (with $h' \in H$). Observe that

$$bh' = gh_2^{-1}h' = ah_1h_2^{-1}h' \in bH$$

because h_1, h_2^{-1}, and h' are all in H and H is a group. Thus $bH \subseteq aH$.

Let c be the number of left cosets of H in G. (The quantity c is finite because G is finite and each element of G is in at most one left coset of H in G.)

Once we show that all cosets have the same number of elements as H has, then we conclude that the order of G is c times the order of H. The function $f : H \to gH$, which sends $h \in H$ to $f(h) = gH$ is a bijection. Indeed, the inverse of f is $f' : gH \to H$ which sends each element θ of

gH to $g^{-1}\theta$. Observe that f' is the inverse of f in the sense that $f' \circ f$ is the identity function on H and $f \circ f'$ is the identity function on gH.

If there is a bijection between two finite sets, then the sets have the same number of elements. $\square$

(2) (5 points) **State Cayley's Theorem.**

Cayley's Theorem. If G is a group, then G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

(3) (8 points) **Let H be a subgroup of $(\mathbb{Z}, +)$. Prove that H is a cyclic group. (Please give a complete proof of the result using the notation of $(\mathbb{Z}, +)$. "We proved a more general statement in class" is not an acceptable answer.)**

If $H = \{0\}$, then H is cyclic. Henceforth, we show that every non-zero subgroup H of $(\mathbb{Z}, +)$ is cyclic. Let H be a non-zero subgroup of $(\mathbb{Z}, +)$. Observe that there are some positive integers in H. (Indeed, if h is a non-zero element of H, then $-h$ is also in H and one of the numbers $\{h, -h\}$ is positive.) Let s be the smallest positive element in H. We claim that $H = \langle s \rangle$. The inclusion $\supseteq$ is obvious. We prove $\subseteq$. Let h be an arbitrary element of H. Divide s into h. It goes q times (for some integer q) with a remainder of r, for some integer r with $0 \le r \le s-1$. Observe that $r = h - sq \in H$ (because H is a group and h and s are in H). But s is the smallest positive element of H; so r must be zero and $h = sq \in \langle s \rangle$.

(4) **Let H be a subgroup of the group G, let g_0 be a fixed element of G, and**

$$H' = \{g_0 h g_0^{-1} \mid h \in H\}.$$

(a) (5 points) **Prove that H' is a subgroup of G.**

We check that H' is closed. Take $h_1' = g_0 h_1 g_0^{-1}$ and $h_2' = g_0 h_2 g_0^{-1}$ in H' for h_1 and h_2 in H. We see that

$$h_1' h_2' = g_0 h_1 g_0^{-1} g_0 h_2 g_0^{-1} = g_0 h_1 h_2 g_0^{-1}$$

Of course, H is a group; so $h_1 h_2 \in H$ and

$$h_1' h_2' = g_0 (\text{an element of } H) g_0^{-1}$$

is an element of H'.

If $h' = g_0 h g_0^{-1}$ is an element of H', then the inverse of h' is equal to $g_0 h^{-1} g_0^{-1}$, which is also in H' because $h^{-1} \in H$ (since H is a group).

It is obvious that H' is non-empty. Indeed, $\mathrm{id} = g_0 \,\mathrm{id}\, g_0^{-1}$ is in H'.

(b) (4 points) **Exhibit a group isomorphism $\phi : H \to H'$. Prove that your ϕ is an isomorphism.**

Define $\phi : H \to H'$ by $\phi(h) = g_0 h g_0^{-1}$. It is obvious that

$$\phi(h_1 h_2) = g_0 h_1 h_2 g_0^{-1} = g_0 h_1 g_0^{-1} g_0 h_2 g_0^{-1} = \phi(h_1)\phi(h_2).$$

It is obvious that the inverse of ϕ is given by $\xi : H' \to H$ with

$$\xi(h') = g_0^{-1} h' g_0.$$

Observe that ξ is a group homomorphism, $\xi \circ \phi$ is the identity function on H and $\phi \circ \xi$ is the identity function on H'.

(c) (4 points) **Give an example of G, H, and H' with $H \neq H'$.**

Take $G = S_3$, $H = \left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$, $g_0 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, and $H' = \left\{ \text{id}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$. Observe that

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

(5) (8 points) **Let $(G, *)$ be a group and $H = \{g * g * g \mid g \in G\}$. Is H always a subgroup of G? If yes, prove the result. If no, give a counterexample.**

No. Consider S_3. Two elements cube to the identity; the other four elements cube to themselves. So H is

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Lagrange's theorem GUARANTEES that H is not a subgroup of S_3 because 4 does not divide into 6.

(6) (8 points) **List all of the subgroups of U_{12}. Each subgroup should be on your list exactly once. Be sure to explain why you know that you have recorded all of the subgroups.**

The group U_{12} is a CYCLIC group with generator $u = e^{(2\pi i)/12}$. We proved that the subgroups of the cyclic group $G = \langle g \rangle$ of order n are

$$\{\langle g^d \rangle \mid d \text{ is a divisor of } n\}.$$

The subgroups of U_{12} are

$$\begin{aligned}
\langle u^1 \rangle &= \{1, u, u^2, u^3, u^4, u^5, u^6, u^7, u^8, u^9, u^{10}, u^{11}\} = U_{12} \\
\langle u^2 \rangle &= \{1, u^2, u^4, u^6, u^8, u^{10}\} = U_6 \\
\langle u^3 \rangle &= \{1, u^3, u^6, u^9\} = U_4 \\
\langle u^4 \rangle &= \{1, u^4, u^8, \} = U_3 \\
\langle u^6 \rangle &= \{1, u^6\} = U_2 \\
\langle u^{12} \rangle &= \{1\} = U_1
\end{aligned}$$