Exam 2 (Part 2)

Your Name:

Names of Any Collaborators:

Instructions

Answer each of the following questions and then submit your solutions to BbLearn by **11:59pm on Monday, November 2**. You can either write your solutions on paper and then capture your work digitally or you can write your solutions digitally on a tablet (e.g., iPad).

This part of Exam 2 is worth a total of 24 points and is worth 30% of your overall score on Exam 2. Your overall score on Exam 2 is worth 20% of your overall grade. Good luck and have fun!

I expect your solutions to be *well-written, neat, and organized.* Do not turn in rough drafts. What you turn in should be the "polished" version of potentially several drafts.

Feel free to type up your final version. The LaTeX source file of this exam is also available if you are interested in typing up your solutions using LaTeX. I'll gladly help you do this if you'd like.

The simple rules for the exam are:

1. You may freely use any theorems that we have discussed in class, but you should make it clear where you are using a previous result and which result you are using. For example, if a sentence in your proof follows from Theorem 5.35, then you should say so.
2. Unless you prove them, you cannot use any results from the course notes that we have not yet covered.
3. You are **NOT** allowed to consult external sources when working on the exam. This includes people outside of the class, other textbooks, and online resources.
4. You are **NOT** allowed to copy someone else's work.
5. You are **NOT** allowed to let someone else copy your work.
6. You are allowed to discuss the problems with each other and critique each other's work.

I will vigorously pursue anyone suspected of breaking these rules.

You should **turn in this cover page** and all of the work that you have decided to submit. **Please write your solutions and proofs on your own paper.**

To convince me that you have read and understand the instructions, sign in the box below.

Signature:

Good luck and have fun!

Recall that on Part 2 of Exam 1, you proved that if G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. This result is known as **Lagrange's Theorem**. Also, recall that if $g \in G$, then $\langle g \rangle \leq G$. Since $|g| = |\langle g \rangle|$, a special case of Lagrange's Theorem says that $|g|$ divides $|G|$ whenever G is finite. You may freely use these results on this exam.

The following information is needed for some of the problems that follow. Let G be a group and $H \leq G$. For each $a \in G$, define

$$aH := \{ah \mid h \in H\}$$

and

$$Ha := \{ha \mid h \in H\}.$$

These sets are called the **left** and **right cosets of H containing** a, respectively. On Part 2 of Exam 1, you also encountered the right cosets. We proved that the right cosets form a partition of G (and used this fact to prove Lagrange's Theorem) and that the right cosets coincide with the clones of H in the Cayley diagram for G. The left cosets also form a partition of G, but they may or may not agree with the clones. That is, the left and right cosets may or may not be equal. Certainly, if G is abelian, then the left and right cosets will coincide. However, if G is not abelian, sometimes the left and right cosets agree and sometimes they do not. For example, consider the dihedral group D_4. It is easy to verify that the left cosets of $\langle s \rangle$ are different from the right cosets of $\langle s \rangle$. In particular, observe that $r\langle s \rangle = \{r, rs\}$ while $\langle s \rangle r = \{r, sr\}$. However, it turns out that the left and right cosets of $\langle r \rangle$ are the same. In this case, the left and right cosets end up being $\{e, r, r^2, r^3\}$ and $\{s, sr, sr^2, sr^3\}$.

The situation where the left and right cosets of H coincide is special. If $aH = Ha$ for all $a \in G$, then H is called a **normal subgroup**, and we write $H \trianglelefteq G$. For example, $\langle s \rangle$ is not normal in D_4, but $\langle r \rangle$ is normal in D_4.

Suppose $(G, *)$ and $(H, \circ)$ are groups. Define $\star$ on $G \times H$ via $(g_1, h_1) \star (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$. This looks fancier than it is. We're just doing the operation of each group in the appropriate component. It is straightforward to prove that $(G \times H, \star)$ is a group. Let's take this for granted. Note that $G \times H$ is called the **direct product** of G and H. Here are some facts about direct products of groups, each of which is easy to prove:

- If e_G and e_H are the identity elements of G and H, respectively, then (e_G, e_H) is the identity element in $G \times H$.
- If $(g, h) \in G \times H$, then $(g, h)^{-1} = (g^{-1}, h^{-1})$.
- The group $G \times H$ is finite if and only if G and H are finite.
- If G and H are finite, then $|G \times H| = |G| \cdot |H|$.
- $G \times H \cong H \times G$.
- The group $G \times H$ is abelian if and only if G and H are abelian.
- If $K \leq G$ and $L \leq H$, then $K \times L \leq G \times H$. However, it is not necessarily true that every subgroup of $G \times H$ is of this form.

We can naturally form direct products of any finite collection of groups. For example, if G, H, and K are groups, then we can form the direct product $G \times H \times K$, where we use the respective operation in each component.

1. (4 points) Prove one of the following theorems.

   Theorem 1 (Theorem 4.44)**.** If G is a finite cyclic group with generator g such that $|G| = n$, then for all $m \in \mathbb{Z}$, $|g^m| = \dfrac{n}{\gcd(n, m)}$.*

   Theorem 2 (Theorem 4.45)**.** If G is a finite cyclic group with generator g such that $|G| = n$, then $\langle g^m \rangle = \langle g^k \rangle$ if and only if $\gcd(m, n) = \gcd(k, n)$.†

2. (2 points each) For each of the following groups, find a generating set and then construct a Cayley diagram using your generating set.

   (a) $\mathbb{Z}_4 \times \mathbb{Z}_2$
   (b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
   (c) $\mathbb{Z}_3 \times \mathbb{Z}_2$

3. (2 points each) Answer each of the following questions.

   (a) Determine whether $\mathbb{Z}_4 \times \mathbb{Z}_2$ is isomorphic to any of D_4, $\mathbb{Z}_8$, Q_8, and L_3. Justify your answer.
   (b) Determine whether $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to any of D_4, $\mathbb{Z}_8$, Q_8, and L_3. Justify your answer.
   (c) Determine whether $\mathbb{Z}_3 \times \mathbb{Z}_2$ is isomorphic to either of $\mathbb{Z}_6$ or D_3. Justify your answer.

4. (4 points each) Prove **two** of the following theorems.

   Theorem 3. Suppose $(G_1, *)$ and $(G_2, \circ)$ are groups and the function $\phi : G_1 \to G_2$ satisfies the homomorphic property. If $g \in G_1$ such that g has finite order, then $|\phi(g)|$ divides $|g|$.

   Theorem 4. Suppose G and H are groups and let $(g, h) \in G \times H$. If $|g|$ and $|h|$ are finite, then $|(g, h)| = \text{lcm}(|g|, |h|)$.

   Theorem 5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

   Theorem 6. Suppose G is a group and let $H \leq G$. If $gHg^{-1} \subseteq H$ for all $g \in G$, then $H \trianglelefteq G$, where $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$.

It turns out that the converse of Theorem 6 is also true. That is, $H \trianglelefteq G$ if and only if $gHg^{-1} \subseteq H$ for all $g \in G$. The set gHg^{-1} is often called the **conjugate of H by g**. Another way of thinking about normal subgroups is that they are "closed under conjugation." It's not too hard to show that if $gHg^{-1} \subseteq H$ for all $g \in G$, then we actually have $gHg^{-1} = H$ for all $g \in G$. This implies that $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for all $g \in G$. This seemingly stronger statement is sometimes used as the definition of normal subgroup.

*By Corollary 4.20, the order of g^m is the smallest positive exponent k such that $(g^m)^k = e$. First, verify that $k = \frac{n}{\gcd(n,m)}$ has the desired property and then verify that it is the smallest such exponent.

†Use Theorem 1 for the forward implication. For the reverse implication, first prove that for all $m \in \mathbb{Z}$, $\langle g^m \rangle = \langle g^{\gcd(m,n)} \rangle$ by proving two set containments. To show $\langle g^m \rangle \subseteq \langle g^{\gcd(m,n)} \rangle$, use the fact that there exists an integer q such that $m = q \cdot \gcd(m, n)$. For the reverse containment, you may freely use a fact known as Bezout's Lemma, which states that $\gcd(m, n) = nx + my$ for some integers x and y.

