Exam 2 (Take-Home Portion)

Your Name:

Names of Any Collaborators:

Instructions

This portion of Exam 2 is worth a total of 22 points and is due at the beginning of class on **Friday, November 3**. Your total combined score on the in-class portion and take-home portion is worth 18% of your overall grade.

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!

1. (4 points each) Suppose $(G, *)$ is a finite cyclic group with generator a such that $|G| = n$. Prove **two** of the following.* You may use earlier parts to prove later parts even if you did not prove the earlier parts.

   (a) For all $s \in \mathbb{Z}$, $|a^s| = \dfrac{n}{\gcd(n, s)}$.†

   (b) If $\langle a^s \rangle = \langle a^t \rangle$, then $\gcd(s, n) = \gcd(t, n)$.

   (c) For all $s \in \mathbb{Z}$, $\langle a^s \rangle = \langle a^{\gcd(s,n)} \rangle$.‡

   (d) If $\gcd(s, n) = \gcd(t, n)$, then $\langle a^s \rangle = \langle a^t \rangle$.§

2. Suppose $(G, *)$ is a group and define $P_2(G) := \{x \in G \mid x = g^2 \text{ for some } g \in G\}$. Complete all of parts (b), (d), and (e) and **one** of parts (a) or (c).

   (a) (4 points) Prove that if G is abelian, then $P_2(G)$ is a subgroup of G.

   (b) (2 points) Is $P_2(G)$ a subgroup if G is non-abelian? If the answer is "yes", prove it. If the answer is "no", provide a counterexample.

   (c) (4 points) Define $\phi : G \to P_2(G)$ via $\phi(g) = g^2$. Prove that if G is an infinite cyclic group, then ϕ is an isomorphism.

   (d) (2 points) Find an example of a finite cyclic group G such that the function ϕ from part (c) is *not* an isomorphism. Briefly justify your answer.

   (e) (2 points) Find an example of a finite cyclic group G such that the function ϕ from part (c) is an isomorphism. Briefly justify your answer.

3. (4 points) Suppose $\phi : G_1 \to G_2$ is a function between two groups that satisfies the homomorphic property (but may or may not be 1-1 or onto). Define the set

$$K_\phi := \{g \in G_1 \mid \phi(g) = e_2\},$$

   where e_1 and e_2 are the identities of G_1 and G_2, respectively. It turns out that K_ϕ is always a subgroup of G_1, but you do not need to worry about proving that. Complete **one** of the following.

   (a) Prove that if $K_\phi = \{e_1\}$, then the function ϕ given above is one-to-one.

   (b) Prove that if the function ϕ given above is one-to-one, then $K_\phi = \{e_1\}$.

*All the parts together make up Theorem 6.43.

†*Hint:* By Corollary 6.13, the order of a^s is the smallest positive exponent k such that $(a^s)^k = e$. First, verify that $k = \frac{n}{\gcd(n,s)}$ has the desired property and then verity that it is the smallest such exponent.

‡*Hint:* You need to do two set containment arguments. To show $\langle a^s \rangle \subseteq \langle a^{\gcd(s,n)} \rangle$, use the fact that there exists an integer q such that $s = q \cdot \gcd(s, n)$. For the reverse containment, you may freely use a fact known as Bezout's Lemma, which states that $\gcd(s, n) = nx + sy$ for some integers x and y.

§*Hint:* Use part (c) a couple of times.

 Written by D.C. Ernst