MATH 4573: HOMEWORK 5

INSTRUCTOR: TYLER GENAO

Due: February 20, 2026.

This homework has two sections: the first section has the assigned problems that you will turn in to Gradescope for credit. The second section contains recommended and bonus problems, either from myself, the textbook or other sources. These latter problems are not graded for credit, but you may find them to be useful practice and/or interesting!

For any assigned problem in this homework, **you must show all of your work in order to receive full credit. Your solutions can only cite up to Lagrange's Theorem in §2.11 of our notes. Everything else must be proven.**

An extra warning: if you have already taken a course in abstract algebra, be careful not to use any results we have yet to prove in class!

1. Problems to Submit

Exercise 1. This exercise proves some routine but important facts about groups. Let G be a group.

a) Show that the identity element $e := e_G$ of G is unique.

Consider an element $g \in G$.

b) Show that if an element $h \in G$ satisfies

$$hg = e,$$

then one also has

$$gh = e,$$

and vice-versa.

c) Show that the inverse g^{-1} of g is unique.

d) Show that $(g^{-1})^{-1} = g$.

e) Show that for any $h \in G$ one has

$$(gh)^{-1} = h^{-1}g^{-1}.$$

f) For an integer $n \geq 0$, we set $g^{-n} := (g^{-1})^n$. Show that for **all** $n \in \mathbb{Z}$, one has

$$g^{-n} = (g^n)^{-1}.$$

Let G' be another group. Consider a group homomorphism

$$\phi \colon G \to G'.$$

g) Show that $\phi(e_G) = e_{G'}$.

h) Show that for any $g \in G$ one has

$$\phi(g^{-1}) = \phi(g)^{-1}.$$

i) Show that for any integer n and an element $g \in G$, one has
$$\phi(g^n) = \phi(g)^n.$$
j) Show that if ϕ is an isomorphism, then so is its inverse map $\phi^{-1}\colon G' \to G$.

Exercise 2. This exercise gives an alternate definition of $\mathbb{Z}/m\mathbb{Z}$, the integers modulo m. In particular, it gives us a new description for the additive group $(\mathbb{Z}/m\mathbb{Z}, +)$, as well as the unit group $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.

Let us define a relation on $\mathbb{Z}$ as follows: say
$$a \sim b$$
when one has
$$a \equiv b \pmod{m}.$$
a) Show that $\sim$ is an *equivalence relation:* i.e., show it is reflexive, symmetric and transitive.
b) For an integer $a \in \mathbb{Z}$, denote its equivalence class under $\sim$ as $[a]$. Describe $[a]$ as a set.
c) Let X be the *quotient set* $\mathbb{Z}/\sim$, i.e., let X be the collection of equivalence classes under $\sim$. Show that X is a group under an addition law $\oplus$ such that
$$(X, \oplus) \cong (\mathbb{Z}/m\mathbb{Z}, +).$$
d) Let $Y \subseteq X$ be the subset of equivalence classes for integers which are coprime to m:
$$Y := \{x \in X : \exists a \in \mathbb{Z} \text{ with } \gcd(a, m) = 1 \text{ and } x = [a]\}.$$
Show that Y is a group under a multiplication law $\odot$ such that
$$(Y, \odot) \cong ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot).$$

Exercise 3.
a) Prove that for $m > 1$, the groups $(\mathbb{Z}/m\mathbb{Z}, +)$ and $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ are never isomorphic.
b) Try to describe the group homomorphisms $(\mathbb{Z}/m\mathbb{Z}, +) \to ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.

Exercise 4. Let G be a group.
a) For an element $g \in G$, prove that if for some $k \in \mathbb{Z}^+$ one has
$$g^k = e,$$
then g has finite order and $|g| \mid k$.
b) Show that if $g \in G$ has finite order, then for all $k \in \mathbb{Z}^+$ one has
$$|g^k| = \frac{|g|}{\gcd(|g|, k)}.$$
Deduce that $|g^k| = |g|$ if and only if $\gcd(|g|, k) = 1$.
c) Prove that for each integer $m \in \mathbb{Z}^+$, the additive group $(\mathbb{Z}/m\mathbb{Z}, +)$ is cyclic with $\varphi(m)$ generators.
d) Assuming that the unit group $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic, prove it has $\varphi(\varphi(m))$ generators.

Exercise 5. Let G be an abelian group.

a) Show that for any elements $a, b \in G$, one has for each $n \in \mathbb{Z}$ that
$$(ab)^n = a^n b^n.$$
b) Show that if $a, b \in G$ have finite orders, then so does ab, and
$$|ab| \mid \operatorname{lcm}(|a|, |b|).$$
c) Show that if $a, b \in G$ have finite *coprime* orders, then
$$|ab| = |a| \cdot |b|.$$

(*Hint:* for parts b) and c), you will want to apply Exercise 4.)

Exercise 6. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From [NZM91, §2.10], pages 119–120: $\#1 - 2, 7 - 8$.
From [NZM91, §2.11], pages 126–127: $\#1 - 6, 12$.

Bonus Exercise 7. Prove that the groups $(\mathbb{Z}/6\mathbb{Z}, +)$ and $((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)$ are isomorphic by giving an explicit isomorphism, writing down where each element goes.

Bonus Exercise 8. In this exercise, let G and G' be finite groups and $\phi\colon G \to G'$ a homomorphism.

a) Given an element $g \in G$, show the order divisibility $|\phi(g)| \mid |g|$.
b) Show that if ϕ is surjective, then for all $g' \in G'$ one has $|g'| \mid |G|$.
c) Give an example of a nontrivial surjective group homomorphism $\phi\colon G \to G'$ where, for some $g \in G$, one has $|\phi(g)| < |g|$.
d) Show that if ϕ is injective, then $|\phi(g)| = |g|$. In particular, injective homomorphisms preserve orders of elements.

Bonus Exercise 9. This exercise will give examples of nonabelian groups. For each integer $n \in \mathbb{Z}^+$, let $\mathrm{Mat}_{n\times n}(\mathbb{R})$ denote the set of $n \times n$ matrices with real entries.

a) Check that $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is an abelian group under matrix addition.
b) Explain why $\mathrm{Mat}_{n\times n}(\mathbb{R})$ is *not* a group under matrix multiplication.
c) Define $\mathrm{GL}_n(\mathbb{R})$, the *general linear group of $n \times n$ matrices,* as the subset of invertible matrices in $\mathrm{Mat}_{n\times n}(\mathbb{R})$. Convince yourself that $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication.
d) Show that $\mathrm{GL}_n(\mathbb{R})$ is abelian if and only if $n = 1$. What is $\mathrm{GL}_1(\mathbb{R})$ isomorphic to, as a group?

References

[NZM91] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th Ed., John Wiley & Sons, Inc., New York (1991).