MATH 4573: HOMEWORK 5

INSTRUCTOR: TYLER GENAO

Due: February 23, 2024.

This homework has two sections: the first section has the problems that you'll turn in for credit. The second section contains recommended problems from the textbook, myself or other sources; you are not required to do these, but I recommend that you check them out.

For any problem in this assignment, **you must show all of your work in order to receive full credit.** Please do not use words such as "clear", "obvious" or "trivial" in your solutions.

Your solutions should not use theorems from sections which come after the day the homework was assigned. This HW can use what we've covered in class so far, including all of §2.11.

A warning: if you've already taken a course in abstract algebra, be careful not to use any results we haven't proven in class!

1. Problems to Submit

Exercise 1. This exercise will explore a "residue system-free" definition of the ring of integers modulo m. Consequently, this alternative definition also applies to the additive group $(\mathbb{Z}/m\mathbb{Z}, +)$, as well as the unit group $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.

Fix an integer $m > 0$. Let us define a relation on $\mathbb{Z}$ as follows: say $a \sim b$ if $a \equiv b \pmod{m}$.

a) Show that $\sim$ is an *equivalence relation:* i.e., show it it reflexive, symmetric and transitive.
b) Given an integer $a \in \mathbb{Z}$, what is the equivalence class $[a]$ of a under $\sim$, explicitly?
c) Using the ring operations $+$ and $\cdot$ from $\mathbb{Z}$, show that the set $\mathbb{Z}/m\mathbb{Z}$ of equivalence classes is also a ring. How many elements does it have?
d) Show that with this definition, $\mathbb{Z}/m\mathbb{Z}$ is isomorphic as a ring to the complete residue system $C(m) := \{0, 1, 2, \ldots, m-1\}$ given in class.

Exercise 2. Prove that the groups $(\mathbb{Z}/4\mathbb{Z}, +)$ and $((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$ are isomorphic via an explicit bijective homomorphism, describing where each element goes. (*Hint:* 2 is a primitive root modulo 5. See HW 3, Exercise 7 for a definition of a primitive root, or §2.8.)

Exercise 3.

a) Prove that the groups $(\mathbb{Z}/m\mathbb{Z}, +)$ and $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ cannot be isomorphic for $m > 1$.
b) Characterize all group homomorphisms $(\mathbb{Z}/m\mathbb{Z}, +) \to ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$.

Exercise 4. In the following, we let G denote a group.

a) Let $g \in G$. Prove that if for $k \in \mathbb{Z}$ 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 $\phi(m)$ generators.
d) Assume that the unit group $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic. Prove that it has $\phi(\phi(m))$ generators.

Exercise 5.

a) Show that for any abelian group G, if $a, b \in G$ have finite order, then so does ab, and the order of ab satisfies

$$|ab| \mid \operatorname{lcm}(|a|, |b|).$$

b) Show that if $|a|$ and $|b|$ are coprime, then $|ab| = |a| \cdot |b|$.

Exercise 6. In the following, we let R denote a ring, with its two operations written as $+$ and $\cdot$.

a) Let $0 := 0_R$ denote the additive identity of R. Show that for all $r \in R$, one has $r \cdot 0 = 0 \cdot r = 0$.
b) Let $1 := 1_R$ denote the multiplicative identity of R. Prove there exists exactly one ring homomorphism $\iota \colon \mathbb{Z} \to R$.
c) Continuing part b), show that ι is injective if and only if 1_R has infinite additive order.
d) Continuing part c), show that if ι is not injective, then *assuming that R is an integral domain,* the additive order of 1_R is prime. (For the definition of an integral domain, see Exercise 7.)

When ι is injective, we say that R has *characteristic zero.* When ι is not injective, we say that R has *positive characteristic p,* where p is the additive order of 1_R.

Exercise 7. Let R be a ring. Say that an element $r \in R$ is a *zero divisor* if for some nonzero $s \in R$ we have $rs = 0$. We say that R is an *integral domain* if R has no nontrivial zero divisors.

a) Show that an integral domain R satisfies the *cancellation property:* for $r, s, t \in R$ with $r \neq 0$, if $rs = rt$ then $s = t$.
b) Show that a field is automatically an integral domain.
c) Give an example of a ring which is not an integral domain, and an integral domain which is not a field.

Exercise 8. Who did you consult for this assignment? What resources did you use?

2. Other Recommended Problems

From the textbook, pages $119 - 120$: $\#1, 2, 7, 8$.
Pages $126 - 127$: $\#1 - 4, 6, 7, 12, 14 - 16, 19$.

Bonus Exercise 9. Characterize the $m \in \mathbb{Z}^+$ for which $\mathbb{Z}/m\mathbb{Z}$ is an integral domain.

Bonus Exercise 10. In this exercise, let G and H be finite groups, and $\varphi\colon G \to H$ a homomorphism.

a) Given an element $g \in G$, show the order divisibility $|\varphi(g)| \mid |g|$.
b) As it turns out, if φ is surjective, then for all $h \in H$ one has $|h| \mid |G|$. Give an example of a nontrivial surjective group homomorphism $\varphi\colon G \to H$ where, for some $g \in G$, one has $|\varphi(g)| < |g|$.
c) Show that if φ is injective, then $|\varphi(g)| = |g|$. In particular, injective homomorphisms and isomorphisms preserve orders.

Bonus Exercise 11. 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 $\mathrm{Mat}_{n\times n}(\mathbb{R})$. Check 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?

Bonus Exercise 12 (Examples of rings)**.** For each set R below, determine whether:

1. R is a ring;
2. R is commutative;
3. R is an integral domain;
4. R is a field.

If R is a ring, then determine its group of units $R^\times$ if possible.

a) The set $\mathbb{Z}[x]$ of polynomials with integer coefficients.
b) The set $C([0,1])$ of continuous real-valued functions $f\colon [0,1] \to \mathbb{R}$.
c) For $n \in \mathbb{Z}^+$, the set $\mathrm{Mat}_{n\times n}(\mathbb{R})$ of $n \times n$ matrices with real entries.
d) For $n \in \mathbb{Z}^+$, the set $\{c_0 + c_1 x + \ldots + c_n x^n : c_i \in \mathbb{Z}\}$ of degree $\leq n$ polynomials over $\mathbb{Z}$.
e) The set of Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.
f) The set of squares of rational numbers, $\{\frac{a^2}{b^2} : a, b \in \mathbb{Z}, b \neq 0\}$.
g) The set of real-valued functions $f\colon \mathbb{R} \to \mathbb{R}$ with $\lim_{x\to 0} f(x) = 0$.

Bonus Exercise 13. Prove that for any prime $p > 2$, writing

$$1 + \frac{1}{2^3} + \ldots + \frac{1}{(p-1)^3} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}$, one has $p \mid a$. (*Hint:* Interpret this sum modulo p, and use the identity $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.)

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).