Math 412 Fall 2022 Midterm Exam

Time: 120 mins.

(a) Answer each question in the space provided. If you require more space, you may use the blank page at the end of this exam, but you must clearly indicate in the provided answer space that you have done so.

(b) You may use any results proved in class, on the homework, or in the textbook, except for the specific question being asked. You should clearly state any facts you are using.

(c) Remember to show all your work.

(d) No calculators, notes, or other outside assistance allowed.

Best of luck!

uniqname: _____

ID number: _____

Question	Points	Score
1	12	
2	15	
3	12	
4	9	
5	20	
6	17	
7	15	
Total:	100	

1. (12 points) Write complete, precise definitions for, or precise mathematical characterizations of, each of the following italicized terms. Be sure to include any quantifiers as needed.

   (a) The *greatest common divisor* of two integers a, b with a, b not both 0 is

   Solution: is the largest integer d such that $d|a$ and $d|b$.

   (b) Let R and S be rings. A ring homomorphism $\varphi\colon R \to S$ is *injective* if

   Solution: for all $r_1, r_2 \in R$, if $\varphi(r_1) = \varphi(r_2)$ then $r_1 = r_2$.

   (c) Let R be a ring. A subset $S \subseteq R$ is a *subring* if

   Solution: S is a ring (and thus, nonempty!) with the same operations $+, \times$ restricted to S, and the same (additive and multiplicative) identities as R.

   (d) Let R be a ring. An ideal $I \subseteq R$ is *prime* if

   Solution: For all x, y in R, if $xy \in I$ then either $x \in I$ or $y \in I$.

2. (15 points) In this problem, you do not need to justify your answers. Give an example of...

(a) a ring R in which not every ideal is principal

Solution: $\mathbb{Z}[x]$ is such a ring, with the ideal $(2, x)$ ()or indeed, (n, x) for any $n \in \mathbb{Z} \neq \pm 1$).
Another, less familiar example is $\mathbb{R}[x, y]$, the set of all polynomials in two variables with coefficients in $\mathbb{R}$.

(b) a ring R with finitely many elements that is not commutative

Solution:

(c) a ring R and an idempotent element $e \in R$ where $e \neq 0_R, 1_R$

Solution: Let R be $\mathbb{Z}_6$ and $e = [3]_6$.

(d) a nilpotent element x in $\mathbb{Z}_{72}$

Solution:

(e) a nonzero zero-divisor a in the quotient ring $\mathbb{Z}_7[x]/(x^2 + x + 1)$

Solution: $x^2 + x + 1 = (x - 2)(x - 4)$ so $(x - 2) = (x + 5)$ or $(x - 4) = (x + 3)$ or any degree 1 multiple of those.

3. (12 points) For each of the statements below, indicate clearly if the statement is TRUE or FALSE. Give a brief, one-sentence justification.

   (a) The ideal $((x-1)(x+2), x(x+2)) \subset \mathbb{Q}[x]$ is a *not* principal ideal.

   Solution:

   (b) Fix two integers a, b with a and b not both 0. Then for all $r, s \in \mathbb{Z}$, we have $ar + bs = \gcd(a, b)$.

   Solution:

   (c) Let a, b, N be integers and assume $N > 0$. If the equation $[a]_N x = [b]_N$ has a solution in $\mathbb{Z}_N$, then the equation $ax = b$ has a solution in $\mathbb{Z}$.

   Solution:

   (d) There exists a solution $x \in \mathbb{Z}$ to the system of equations

$$\begin{cases} x \equiv 7 \pmod{23} \\ x \equiv 4 \pmod{87} \end{cases}$$

   Solution: There is a solution! By Bézout's identity, there exists $r, s \in \mathbb{Z}$ such that $23r + 87s = 1$. Thus $[23r]_{87} = [1]_{87}$, so $[4 \cdot 23 \cdot r]_{87} = [4]_{87}$. Similarly, $[87s]_{23} = [1]_{23}$, so $[7 \cdot 87 \cdot s]_{+23} = [7]_{23}$. Combining gives that

$$4 \cdot 23r + 7 \cdot 87s$$

   is such a solution.
   In fact, $-34 \cdot 23 + 9 \cdot 87$, so

$$\begin{aligned} x &= 4 \cdot 23 \cdot -34 + 7 \cdot 87 \cdot 9 \\ &= 2353 \end{aligned}$$

   is a specific solution.

4. (9 points) Solve the following problems and justify your reasoning.

   (a) How many units are in $\mathbb{Z}_{64}$?

   Solution: 32

   (b) Find a congruence class $[a]_{64}$ such that $[a]_{64}x = [0]_{64}$ has exactly 4 distinct solutions in $\mathbb{Z}_{64}$.

   Solution: Any congruence class $[a]_{64}$ such that $\gcd(a, 64) = 4$:

   $$[4]_{64}, [12]_{64}, [20]_{64}, [28]_{64}, [36]_{64}, [44]_{64}, [52]_{64}, [60]_{64}$$

   (c) Find a multiplicative inverse of $1 + 8x$ in $\mathbb{Z}_{64}[x]$.

   Solution:

   $$1 - 8x$$

   or equivalently

   $$1 + 56x$$

5. (20 points) For $n \in \mathbb{Z}$, consider the two families of rules

$$\varphi_n \colon \mathbb{Z}_{12} \to \mathbb{Z}_{60}, \qquad [a]_{12} \mapsto [na]_{60}$$
$$\psi_n \colon \mathbb{Z}_{60} \to \mathbb{Z}_{12}, \qquad [a]_{60} \mapsto [na]_{12}$$

(a) Prove that φ_n is a well-defined function if and only if $5 \mid n$.

Solution: If φ_n is well-defined, then for all $a, b \in \mathbb{Z}$, if $a \equiv b \mod 12$, then $na \equiv nb \mod 60$. In particular, $a = 0$ and $b = 12$, then $0 \equiv 12n \mod 60$, so $60|12n$. That is, there exists some $k \in \mathbb{Z}$ such that $60k = 12n$, which implies that $5k = n$. Thus $5|n$.

(b) For which $n \in \mathbb{Z}$ is φ_n a ring homomorphism? Prove your assertion.

Solution: No such n. In order to be a ring homomorphism, the function must be well-defined and $\varphi([1]_{12}) = [1]_{60}$. From part (a), in order for φ to be well-defined, n must be divisible by 5.
But if $5|n$, then $[n]_{60}$ will not be equal to $[1]_{60}$.
To see this, notice that if $[n]_{60} = [1]_{60}$ then $60|n-1$, so $5|n-1$. But then it could not be that $5|n$.

(c) Prove that for any $n \in \mathbb{Z}$, the rule ψ_n is a well-defined function.

Solution:

(d) Find all $n \in \mathbb{Z}$ for which ψ_n is a ring homomorphism? You do not need to prove your assertion.

Solution: Whenever n is congruent to 1 mod 12.

6. (17 points) Consider the polynomial $f(x) = x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ and let I be the ideal in $\mathbb{Z}_5[x]$ generated by $f(x)$.

   (a) Prove that $f(x)$ is irreducible in $\mathbb{Z}_5[x]$.

Solution:

$a \in \mathbb{Z}_5$	$f(a)$
0	2
1	2
2	2
3	3
4	1

By exhaustion, $f(x)$ has no roots in $\mathbb{Z}_5$. We showed in class that if a degree 3 polynomial has no roots, then it is irreducible.

   (b) Circle one of the three phrases below to complete the following sentence:

The quotient ring $Q = \mathbb{Z}_5[x]/I$ is

a) a ring but not a domain. b) a domain but not a field. c) a field.

Briefly justify your choice.

Solution:

a) a ring but not a domain. b) a domain but not a field.

c) a field.

Consider the polynomial $f(x) = x^3 + 2x^2 + 2x + 2 \in \mathbb{Z}_5[x]$ and let I be the ideal in $\mathbb{Z}_5[x]$ generated by $f(x)$.

(c) There exist $a, b, c \in \mathbb{Z}_5$ such that $2x^3 + x + I = ax^2 + bx + c + I$. Find a, b, c.

$a =$ _____ $b =$ _____ $c =$ _____

Solution:

$$a = 1 \qquad b = 2 \qquad c = 1$$

(d) How many elements are in Q? You do not need to justify your answer.

Solution: $125 = 5^3$

(e) Let N be the number of elements in Q. Prove that Q is *not* isomorphic to $\mathbb{Z}_N$.

Solution: Not only is Q is not isomorphic to $\mathbb{Z}_N$, but there does not exist a homomorphism from Q to $\mathbb{Z}_N$!
To see this, suppose that φ were a homomorphism from Q to $\mathbb{Z}_N$. Then $\varphi([1]_5) = [1]_{125}$. But then

$$\begin{aligned}\varphi([0]_5) &= \varphi\Big([1]_5 + [1]_5 + [1]_5 + [1]_5 + [1]_5\Big) \\ &= [1]_{125} + [1]_{125} + [1]_{125} + [1]_{125} + [1]_{125} \\ &= [5]_{125} \\ &\neq [0]_{125}\end{aligned}$$

Ring homomorphisms always map 0 to 0 (we showed this on a worksheet), so this is a contradiction.

7. (15 points) Let $S \subset \mathbb{Q}$ be the subset of rational numbers with odd denominators (when expressed in lowest terms).

   (a) Show that S is a subring of $\mathbb{Q}$

Solution:

- S is non-empty and contains $1 = \frac{1}{1}$ and $0 = \frac{0}{1}$.
- **closed under addition:** Suppose $\frac{a}{b}, \frac{c}{d}$ are in S. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

  This fraction might not be in lowest terms; however, if it can be written in lowest terms as $\frac{e}{f}$ for some integers e, f, then

$$ebd = f(ad + bc)$$

  . Since $\gcd(e, f) = 1$, this implies that f divides bd. Given that both b and d are odd, we know that $2 \not| bd$. Thus it cannot be that $2|f$. Regardless of what the sum is in lowest terms, the denominator is odd.

- **closed under multiplication:**Suppose $\frac{a}{b}, \frac{c}{d}$ are in S. Then

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

  Again, this fraction might not be in lowest terms, but since bd is odd, if $\frac{ac}{bd} = \frac{e}{f}$ written in lowest terms, f is odd.

- **contains additive inverses:** Suppose $\frac{a}{b}$ is in S and is written in lowest terms (so $\gcd(a, b) = 1$). Then b is odd. So $\frac{-a}{b}$ is also in lowest terms (because $\gcd(-a, b) = 1$ as well), meaning that $\frac{-a}{b}$ is in S.

.

   (b) Consider the map $\varphi\colon S \to \mathbb{Z}_2$ to be the ring homomorphism defined by

$$\varphi\left(\frac{r}{s}\right) = [r]_2,$$

   where $\frac{r}{s}$ is in lowest terms. (You do not need to show that φ is a ring homomorphism.) Let $I \subseteq S$ be the subset of rational numbers with even numerator (when expressed in lowest terms). Prove that I is an ideal of S.

Solution: We show that $I = \ker(\varphi)$ and use the fact that kernels of homomorphisms are ideals.
$\subseteq$: Suppose $\frac{a}{b} \in I$, written in lowest terms. Then a is even, so $[a]_2 = [0]_2$. Thus $\frac{a}{b}$ is in $\ker(\varphi)$.
$\supseteq$ Suppose $\frac{a}{b} \in \ker(\varphi)$, written in lowest terms. Then $[a]_2 = [0]_2$, so $2|a$. Thus $\frac{a}{b}$ is in I.

(c) Prove that φ is surjective and that $S/I \cong \mathbb{Z}_2$.

Solution: As we proved in part a, $\frac{0}{1}, \frac{1}{1} \in S$. Evaluating, we see that $\varphi(\frac{0}{1}) = [0]_2$ and $\varphi(\frac{1}{1}) = [1]_2$. Therefore φ is surjective.
Using Noether's first isomorphism theorem and the fact that $I = \ker \varphi$, we immediately have that $S/I \cong \mathbb{Z}_2$.

You can use this space for work.

You can use this space for work.