

Department of Mathematics, University of Wisconsin-Madison
Math 541 — Final Exam — Solutions — Fall 2025

NAME :

EMAIL:

@wisc.edu

Question	Points	Score
1	10	
2	18	
3	9	
4	5	
5	5	
6	6	
7	8	
8	6	
9	6	
Total:	73	

INSTRUCTIONS:

Time: **120 minutes**

- This exam contains 9 questions some with multiple parts, 10 pages (including the cover) for the total of 73 points. Read the problems carefully and budget your time wisely.
- **NO CALCULATORS** or other electronic devices are to be used. Turn off your phone so as to not disturb others. **NO NOTES OR BOOKS** of any sort to be used too.
- Please present your solutions in a clear manner. Cross out any writing that you do not wish to be graded.
- Unless otherwise specified, you must justify your claims and use complete sentences (or at least logical connectors indicating what you are assuming and what you are deducing).
- If you use an additional page for a particular problem, be sure to **CLEARLY** indicate this on the problem's page so I know to look further. Ask for more scratch paper if needed. All scratch papers must be submitted as well.
- Please write your name on every page.

Some definitions

$$\begin{aligned}Z(G) &= \{g \in G \mid gx = xg \text{ for all } x \in G\} = \{g \in G \mid gxg^{-1} = x \text{ for all } x \in G\}, \\C_G(A) &= \{g \in G \mid ga = ag \text{ for all } a \in A\} = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}, \\N_G(A) &= \{g \in G \mid gA = Ag\} = \{g \in G \mid gAg^{-1} = A\}, \\G_s &= \{g \in G \mid g \cdot s = s\}.\end{aligned}$$

1. (10 points) TRUE/FALSE, no justifications needed.

(a) The two additive groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ are isomorphic.

☒ **TRUE**

☐ **FALSE**

(b) Let R be a ring. Every prime ideal of R is a maximal ideal.

☐ **TRUE**

☒ **FALSE**

(c) Let G be a group. For any nonempty set $A \subseteq G$, we have the center of G is a subset of the centralizer of A , i.e. $Z(G) \subseteq C_G(A)$.

☒ **TRUE**

☐ **FALSE**

(d) Let R be a ring, and let A and B be ideals of R . Then $\{ab \mid a \in A, b \in B\}$ is an ideal of R .

☐ **TRUE**

☒ **FALSE**

(e) Let R be a ring, and let A and B be ideals of R . Then $\{a + b \mid a \in A, b \in B\}$ is an ideal of R .

☒ **TRUE**

☐ **FALSE**

2. (18 points) Consider each ideal in the corresponding ring. Circle all properties which holds. An ideal may be more than one.

(a) (7) in $\mathbb{Z}/49\mathbb{Z}$

- ☒ Maximal ideal
☒ Prime ideal
☒ Principal ideal
☐ Non of above

(b) $(10, 22)$ in $\mathbb{Z}$,

- ☒ Maximal ideal
☒ Prime ideal
☒ Principal ideal
☐ Non of above

(c) $(2, 2^2, 2^{2^2}, \dots)$ in $\mathbb{Z}$

- ☒ Maximal ideal
☒ Prime ideal
☒ Principal ideal
☐ Non of above

(d) (5) in $\mathbb{Z}[x]$

- ☐ Maximal ideal
☒ Prime ideal
☒ Principal ideal
☐ Non of above

(e) (0) in $\mathbb{R}[x]$,

- ☐ Maximal ideal
☒ Prime ideal
☒ Principal ideal
☐ Non of above

(f) $(2, x^2 + x)$ in $\mathbb{R}[x]$

- ☐ Maximal ideal
☐ Prime ideal
☒ Principal ideal
☐ Non of above

3. (9 points) ANSWER ONLY, no justifications needed.

(a) Give an example of a ideal I in $\mathbb{Q}[x]$ such that

- $I \neq (0)$,
- $I \neq \mathbb{Q}[x]$,
- I is not maximal.

Solution: (x^2) .

(b) Give an example of I and J in a ring R where $IJ \neq I \cap J$.

Solution: $R = \mathbb{Z}$, $I = 2\mathbb{Z}$, $J = 4\mathbb{Z}$.

(c) Write down examples of non-abelian groups of orders 6, 8, and 12.

Solution: D_6 or S_3 or $GL_2(\mathbb{F}_2)$; D_8 or Q_8 ; D_{12} or A_4 or $S_3 \times Z_2$,

4. (5 points) Let G be a cyclic group of order 20. How many subgroups does G have?

Solution: G is cyclic, so all subgroups are cyclic. There is unique subgroup of given order in G , and possible orders are divisors of $|G|$. $G \cong \mathbb{Z}/20\mathbb{Z} = \langle 1 \rangle$, so subgroups are

order	generator
1	0
2	10
4	5
5	4
10	2
20	1

Total 6 subgroups.

5. (5 points) Let G, H be groups. Suppose $\varphi : G \rightarrow H$ is a surjective homomorphism. If G is abelian, prove that H must be abelian.

Solution: φ is surjective means for every h_i there is g_i such that $\varphi(g_i) = h_i$. Now to show that $h_1 h_2 = h_2 h_1$ we can write

$$h_1 h_2 = \varphi(g_1) \varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1) = \varphi(g_2) \varphi(g_1) = h_2 h_1.$$

Solution: Using the First Isomorphism Theorem

$$G / \ker(\varphi) = \text{im}(\varphi) = H,$$

so H is a quotient group of G . Now

$$h_1 h_2 = g_1 H g_2 H = g_1 g_2 H = g_2 g_1 H = g_2 H g_1 H = h_2 h_1.$$

6. (6 points) Show that the subring of $M_{2 \times 2}(\mathbb{R})$ consists of matrices

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad a, b \in \mathbb{R}$$

is isomorphic to field of complex numbers $\mathbb{C}$.

Solution: Let's denote this subring S . Consider the map $\varphi : S \rightarrow \mathbb{C}$ which maps

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi.$$

This is ring homomorphism:

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= a + bi + c + di = (a + c) + (b + d)i \\ \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} a + c & b + d \\ -b - d & a + c \end{pmatrix}\right) = a + c + (b + d)i \\ \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) \varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= (a + bi)(c + di) = (ac - bd) + (bc + ad)i \\ \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix}\right) = ac - bd + (ad + bc)i. \end{aligned}$$

We need to check that φ is a bijection. There is a map $\psi : \mathbb{C} \rightarrow S$:

$$\psi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

which is definitely inverse to φ , so φ is the bijection, so isomorphism between S and $\mathbb{C}$.

7. (8 points) Sophus take a ring $(R, +, \cdot)$, and decided to define a new operation bracket: for every $a, b \in R$

$$[a, b] = ab - ba.$$

He claims that R is now a ring with respect to $+$ and bracket.

Write down explicitly which properties we need to check to prove/disprove this claim (you will assigned partial credit for this) and check **all** of them.

Solution: The first operation didn't change, so all properties of addition holds. Now we need to check that

- R is closed under bracket
- bracket is associative:

$$[a, [b, c]] = [[a, b], c]$$

for every $a, b, c \in R$

- bracket is distributive over addition:

$$[a, b + c] = [a, b] + [a, c] \quad \text{and} \quad [a + b, c] = [a, c] + [b, c]$$

for every $a, b, c \in R$

First one is clear, next two needs proof

$$\begin{aligned} [a, [b, c]] &= [a, bc - cb] = a(bc - cb) - (bc - cb)a = abc - acb - bca + cba \\ [[a, b], c] &= [ab - ba, c] = (ab - ba)c - c(ab - ba) = abc - bac - cab + cba \end{aligned}$$

These two expressions are not equal, so we can't claim it holds for any ring. Still it can be true for some non commutative rings.

$$\begin{aligned} [a, b + c] &= a(b + c) - (b + c)a = ab + ac - ba - ca = ab - ba + ac - ca = [a, b] + [a, c] \\ [a + b, c] &= (a + b)c - c(a + b) = ac + bc - ca - cb = ac - ca + bc - cb = [a, c] + [b, c]. \end{aligned}$$

These properties holds for any rings.

8. (6 points) Let R be a commutative ring with $1 \neq 0$. Let $x \in R$, and suppose $x^2 = 0$. Let N denote the intersection of all of the prime ideals in R . Prove that $x \in N$.

Solution: Suppose P is any prime ideal in R . We have $x \cdot x = x^2 = 0 \in R$, so $x \in R$ by the definition of a prime ideal. Now x lie in any prime ideal, so in the intersecion of all prime ideal too.

9. (6 points) Let R be a commutative ring with 1. In lecture, we proved that a maximal ideal M of R must be a prime ideal of R as a corollary of our results on the quotient R/M . Let's prove that "maximal implies prime" in a more direct way, using the definitions.

Let M be a maximal ideal of R . Suppose a and b are elements of R , and that $ab \in M$. Assume that a is not in M . Now we want to prove that $b \in M$. Since M is a maximal ideal and $a \notin M$, the ideal $aR + M$ is strictly bigger than M , and therefore $aR + M = R$.

This means that, for some $r \in R$ and some $m \in M$, we have $ar + m = 1$.

[I spilled a drink on my paper and lost the rest of the proof. You need to finish the equation above and write the rest of the proof.]

Solution: This means that, for some $r \in R$ and some $m \in M$, we have $ar + m = 1$. Next

$$b = 1 \cdot b = (ar + m)b = abr + mb,$$

$ab \in M$, $m \in M$, so $RHS \in M$ and $b \in M$.

SCRATCH PAPER - DO NOT REMOVE FROM YOUR EXAM.
SCRATCH WORK WILL NOT BE GRADED