

Math 300 D - Autumn 2025
Final Exam
December 11, 2025
Solutions

1. Suppose A, B and C are non-empty sets. Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$.

(a) Prove that if f is onto and g is not one-to-one, then $g \circ f$ is not one-to-one.

Suppose A, B, C, f , and g are as introduced above.

Suppose f is onto and g is not one-to-one.

Then there exist $b_1, b_2 \in B$ with $b_1 \neq b_2$ and $g(b_1) = g(b_2)$.

Since f is onto, there exist $a_1, a_2 \in A$, $a_1 \neq a_2$ with $f(a_1) = b_1$ and $f(a_2) = b_2$.

Then $g(f(a_1)) = g(f(a_2))$.

Since $a_1 \neq a_2$, we conclude that $g \circ f$ is not one-to-one. ■

(b) Prove that if f is not onto and g is one-to-one, then $g \circ f$ is not onto.

Suppose A, B, C, f , and g are as introduced above.

Suppose f is not onto and g is one-to-one.

Since f is not onto, there exists a $b_2 \in B$ with b_2 not in the range of f .

Let $z = g(b_2)$.

Suppose there exists $a \in A$ with $g(f(a)) = z$.

Since g is one-to-one, $b_2 = f(a)$, and so b_2 is in the range of f ; this is a contradiction.

Hence, there does not exist $a \in A$ with $g(f(a)) = z$ and so $g \circ f$ is not onto. ■

2. Let A and B be sets. Prove that $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let A and B be sets.

Suppose $A \subseteq B$.

Suppose $S \in \mathcal{P}(A)$, so $S \subseteq A$.

Suppose $x \in S$.

Then $x \in A$, so $x \in B$.

Hence, $x \in S$ implies $x \in B$, so $S \subseteq B$, and so $S \in \mathcal{P}(B)$.

Thus, $S \in \mathcal{P}(A)$ implies $S \in \mathcal{P}(B)$, and hence $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Now, suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Since $A \subseteq A$, we have $A \in \mathcal{P}(A)$.

Hence, $A \in \mathcal{P}(B)$, and so $A \subseteq B$.

Thus, $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. ■

3. Suppose A is a finite set and $b \in A$. Prove that $A \setminus \{b\}$ is finite by demonstrating the necessary bijection. You need not prove it is a bijection.

Suppose A is a finite set and $b \in A$.

Then $A \sim I_n$ for some $n \in \mathbb{Z}_{\geq 0}$ and there exists $f : A \rightarrow I_n$ that is a bijection.

If $A \setminus \{b\} = \emptyset$, then $A \setminus \{b\} \sim I_0$ and hence is finite.

Suppose $A \setminus \{b\} \neq \emptyset$.

Let $k = f(b)$.

Define $g : A \setminus \{b\} \rightarrow I_{n-1}$ by

$$g(x) = \begin{cases} f(x) & \text{if } f(x) < k \\ f(x) - 1 & \text{if } f(x) > k. \end{cases}$$

Then g is a bijection, and so $A \setminus \{b\} \sim I_{n-1}$.

Hence, $A \setminus \{b\}$ is finite. ■

4. (a) Let a be an integer. Prove that if $a \equiv 1 \pmod{2}$, then $a^2 \equiv 1 \pmod{8}$.

Let $a \in \mathbb{Z}$.

Suppose $a \equiv 1 \pmod{2}$.

Then $a = 2k + 1$ for some integer k and we have

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Suppose k is even.

Then $k = 2m$ for some integer m , and $a^2 = 4(2m)(k + 1) + 1 = 8m(k + 1) + 1$.

Hence, $a^2 - 1 = 8m(k + 1)$, and so $a^2 \equiv 1 \pmod{8}$.

Suppose k is odd.

Then $k = 2m + 1$ for some integer m , and $a^2 = 4k(2m + 2) + 1 = 8k(m + 1) + 1$.

Hence, $a^2 - 1 = 8k(m + 1)$ and so $a^2 \equiv 1 \pmod{8}$.

Thus, $a^2 \equiv 1 \pmod{8}$. ■

- (b) Let $m \in \mathbb{Z}, m > 0$.

Suppose $a \equiv b \pmod{m}$ for some integers a and b .

Suppose $d \mid m$ for some positive integer d .

Prove that

$$a \equiv b \pmod{d}.$$

Let m be a positive integer.

Suppose a and b are integers and $a \equiv b \pmod{m}$.

Then $m \mid a - b$, and so $a - b = mk$ for some integer k .

Suppose $d \mid m$ for some positive integer d .

Then $m = ds$ for some integer s .

Hence, $a - b = dsk$, so $d \mid a - b$.

Thus, $a \equiv b \pmod{d}$. ■

5. Use induction to prove the following theorem.

Theorem: Let $n \in \mathbb{Z}$, $n \geq 1$. Then

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} = \sum_{j=1}^n \frac{1}{\sqrt{j}} \geq \sqrt{n}.$$

Proof:

For $n \in \mathbb{Z}$, $n \geq 1$, let $P(n)$ be the statement

$$\sum_{j=1}^n \frac{1}{\sqrt{j}} \geq \sqrt{n}.$$

Base case: Let $n = 1$. Then

$$\sum_{j=1}^1 \frac{1}{\sqrt{j}} = \sum_{j=1}^1 \frac{1}{\sqrt{j}} = \frac{1}{\sqrt{1}} = \frac{1}{1} = 1 \geq \sqrt{1} = \sqrt{n}.$$

So $P(1)$ is true.

Induction step: Suppose $P(k)$ is true for some $k \in \mathbb{Z}_{\geq 1}$.

Then

$$\begin{aligned} \sum_{j=1}^{k+1} \frac{1}{\sqrt{j}} &= \sum_{j=1}^k \frac{1}{\sqrt{j}} + \frac{1}{\sqrt{k+1}} \\ &\geq \sqrt{k} + \frac{1}{\sqrt{k+1}} \quad (\text{by the induction hypothesis}) \\ &= \frac{\sqrt{k}\sqrt{k+1} + 1}{\sqrt{k+1}} \\ &> \frac{\sqrt{k}\sqrt{k} + 1}{\sqrt{k+1}} \\ &= \frac{k+1}{\sqrt{k+1}} \\ &= \sqrt{k+1}. \end{aligned}$$

Hence, $P(k+1)$ is true.

Thus, $P(k)$ implies $P(k+1)$.

Therefore, since $P(1)$ is true, by induction $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 1}$. ■

6. (a) *Prove the following theorem.*

Theorem: *Let A be a non-empty set and suppose R is an equivalence relation on A .*

Suppose $B \subseteq R$ and $C \subseteq R$ are disjoint, i.e., $B \cap C = \emptyset$.

Then B and C cannot both be equivalence relations on A .

Let A, R, B and C be introduced as above.

Suppose B is an equivalence relation.

Let $a \in A$.

Since B is reflexive, $(a, a) \in B$.

Since $B \cap C = \emptyset$, $(a, a) \notin C$.

Hence, C is not reflexive and so C is not an equivalence relation on A .

Thus, B and C cannot both be equivalence relations on A . ■

- (b) *Give a set A and two equivalence relations R and T on A such that $R \subseteq T$ and $R \neq T$.*

You need not prove R and T are equivalence relations.

Let $A = \{1, 2\}$.

Let $R = \{(1, 1), (2, 2)\}$

Let $T = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$.

Elementary Properties of the Integers (EPIs)

Suppose a, b, c , and d are integers.

- **Closure:** $a + b$ and ab are integers.
- **Substitution of Equals:** If $a = b$, then $a + c = b + c$ and $ac = bc$.
- **Commutativity:** $a + b = b + a$ and $ab = ba$.
- **Associativity:** $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.
- **The Distributive Law:** $a(b + c) = ab + ac$
- **Identities:** $a + 0 = 0 + a = a$ and $a \cdot 1 = 1 \cdot a = a$.
 0 is called the additive identity.
 1 is called the multiplicative identity.
- **Additive Inverses:** There exists an integer $-a$ such that $a + (-a) = (-a) + a = 0$.
- **Trichotomy:** Exactly one of the following is true:
 $a > 0$, $-a > 0$, or $a = 0$.
- **The Well-Ordering Principle:** Every non-empty set of positive integers contains a smallest element.

1. $a \cdot 0 = 0$
2. If $a + c = b + c$, then $a = b$.
3. $-a = (-1) \cdot a$
4. $(-a) \cdot b = -(ab)$
5. $(-a) \cdot (-b) = ab$
6. If $ab = 0$, then $a = 0$ or $b = 0$.
7. If $a \leq b$ and $b \leq a$, then $a = b$.
8. If $a < b$ and $b < c$, then $a < c$.
9. If $a < b$, then $a + c < b + c$.
10. If $a < b$ and $0 < c$, then $ac < bc$.
11. If $a < b$ and $c < 0$, then $bc < ac$.
12. If $a < b$ and $c < d$, then $a + c < b + d$.
13. If $0 \leq a < b$ and $0 \leq c < d$, then $ac < bd$.
14. If $a < b$, then $-b < -a$.
15. $0 \leq a^2$, where $a^2 = a \cdot a$.
16. If $ab = 1$, then either $a = b = 1$ or $a = b = -1$.

Sets

$A \subseteq B$ iff $x \in A$ implies $x \in B$

$A = B$ iff $A \subseteq B$ and $B \subseteq A$

$x \in A \cup B$ iff $x \in A$ or $x \in B$

$x \in A \cap B$ iff $x \in A$ and $x \in B$

$x \in A \setminus B$ iff $x \in A$ and $x \notin B$

$\mathcal{P}(A)$ is the set of all subsets of a set A

For a family $\mathcal{F}$:

$$\bigcup \mathcal{F} = \{x : \exists S \in \mathcal{F} \text{ such that } x \in S\}$$

$$\bigcap \mathcal{F} = \{x : \forall S \in \mathcal{F}, x \in S\}$$

NOTE: Properties 8-14 hold if each $<$ is replaced with $\leq$.

Euclid's Division Theorem: For all positive integers m and all integers n , there exist unique integers q and r , with $0 \leq r < m$ such that $n = qm + r$.

Bijections have inverse functions Theorem: Let $f : A \rightarrow B$ be a bijection, where A and B are sets. Then $f^{-1} : B \rightarrow A$ and is a bijection.

Inverse composition Theorem: A function $f : A \rightarrow B$ is a bijection iff there is a function $g : B \rightarrow A$ such that $f \circ g = i_B$ and $g \circ f = i_A$.