Q1. [**5 points**] Carefully prove the following proposition using only the axioms of $\mathbb{Z}$, the properties of $=$, and the definition of subtraction.

Proposition. Let $r, s, t, u \in \mathbb{Z}$. If $r \neq 0$ and $r\big(s - (tu)\big) = t(rs)$, then $s = t(s + u)$.

Clearly indicate your assumptions and make sure to justify each step of your proof by naming one axiom of $\mathbb{Z}$ or by citing "replacement" or "definition of subtraction".
Do NOT use any propositions we proved in class.

Solution: **Proof.** Let $r, s, t, u \in \mathbb{Z}$. Assume $r \neq 0$ and $r(s - tu) = t(rs)$. Then

$$
\begin{aligned}
& r(s - tu) = t(rs) & \\
\implies\ & r(s - tu) = (rs)t & \text{[Commut. of Mult.]} \\
\implies\ & r(s - tu) = r(st) & \text{[Assoc. of Mult.]} \\
\implies\ & (s - tu) = st & \text{[Cancellation } (r \neq 0)\text{]} \\
\implies\ & s + (-tu) = st & \text{[Def. of Subtraction]} \\
\implies\ & (s + (-tu)) + tu = st + tu & \text{[Replacement]} \\
\implies\ & s + ((-tu) + tu) = st + tu & \text{[Assoc. of Add.]} \\
\implies\ & s + (tu + (-tu)) = st + tu & \text{[Commut. of Add.]} \\
\implies\ & s + 0 = st + tu & \text{[Add. Inv. Ax.]} \\
\implies\ & s = st + tu & \text{[Add. Id. Ax.]} \\
\implies\ & s = ts + tu & \text{[Commut. of Mult.]} \\
\implies\ & s = t(s + u) & \text{[Distrib.]}
\end{aligned}
$$

Q2. [**4 points**] Write the negation of each of the following statements. Do not simply write "not" or $\neg$ in front of the statement, i.e. simplify each statement's negation appropriately.

(a) $(\exists\, b \in \mathbb{Q} \text{ such that })(\forall m, n \in \mathbb{Z})\ \left[\frac{m}{n} = b \text{ and } m < n\right]$.

Solution: $(\forall b \in \mathbb{Q})(\exists m, n \in \mathbb{Z} \text{ such that })\ \left[\frac{m}{n} \neq b \text{ or } m \geq n\right]$.

(b) There exist real numbers x, y such that $x^2 > y$ or $y + 1 = x$.

Solution: For all real numbers x, y, $x^2 \leq y$ and $y + 1 \neq x$.

(c) If Moon is barking, then Moon is getting attention.

Solution: Moon is barking and Moon is not getting attention.

(d) $x = 0 \iff (\exists y \in \mathbb{N} \text{ such that })\ y > x$

Solution: $[x = 0 \text{ and } (\forall y \in \mathbb{N})\ y \leq x]$ or $[x \neq 0 \text{ and } (\exists y \in \mathbb{N})\ y > x]$

Alternatively: $x \neq 0 \iff (\exists y \in \mathbb{N} \text{ such that })\ y > x$

or $x = 0 \iff (\forall y \in \mathbb{N})\ y \leq x$

Q3. [**5 points**] Let $a, b \in \mathbb{Z}$ and consider the following implication P:

P: If $5 \mid a$ and $12 \mid (2b + 6)$, then $15 \mid ab$.

(a) Is P true for all $a, b \in \mathbb{Z}$? Fully justify your answer with a proof or counterexample and explanation.

Solution: P is true:

Let $a, b \in \mathbb{Z}$. Assume $5 \mid a$ and $12 \mid (2b+6)$. Then $\exists k, l \in \mathbb{Z}$ such that $a = 5k$ and $2b + 6 = 12l$. Therefore, $2b = 12l - 6$, hence $b = 6l - 3$.

It now follows that $ab = (5k)(6l-3) = (5k)(3)(2l-1) = 15(k(2l-1))$.

Since $k, l, 2 \in \mathbb{Z}$, it follows that $k(2l-1) \in \mathbb{Z}$. Therefore, $15 \mid ab$. □

(b) State the **contrapositive** of P. Is the contrapositive of P true for all $a, b \in \mathbb{Z}$? Fully justify your answer.

Solution: Contrapositive of P:

If $15 \nmid ab$, then $5 \nmid a \quad \text{or} \quad 12 \nmid (2b+6)$.

The contrapositive of P is equivalent to P. Since we proved that P is true, the contrapositive must also be true for all $a, b \in \mathbb{Z}$.

(c) State the **converse** of P. Is the converse of P true for all $a, b \in \mathbb{Z}$? Fully justify your answer.

Solution: Converse of P: If $15 \mid ab$, then $5 \mid a$ and $12 \mid (2b+6)$.

The converse of P can be false:

Let $a = 3$ and $b = 5$. Then $ab = 15$ so $15 \mid ab$ but $5 \nmid 3$ and $12 \nmid (2(5)+6)$

Q4. [**5 points**] Consider the infinite integer sequence $(x_n)_{n=0}^{\infty}$ defined recursively, as follows:

$$x_0 = 1$$
$$\text{for all } n \in \mathbb{N}, \quad x_n = x_{n-1} + (2n+1)^2$$

Use a **proof by induction** to show that $x_n = \dfrac{(n+1)(2n+1)(2n+3)}{3}$ for all $n \in \mathbb{N}$.

Your proof must be well-organized and each step must be appropriately justified. Clearly state your induction hypothesis and indicate "by IH" when it is used in your induction step.

Solution: For each $n \in \mathbb{N}$, let $P(n)$ be the statement $x_n = \frac{(n+1)(2n+1)(2n+3)}{3}$

base cases For $n = 1$, we have

$$x_1 = x_0 + (2(1)+1)^2 = 1 + 3^2 = 10$$

and

$$\frac{(n+1)(2n+1)(2n+3)}{3} = \frac{(1+1)(2(1)+1)(2(1)+3)}{3} = \frac{2(3)(5)}{3} = 10$$

Thus, $P(1)$ holds.

Ind. Hyp. Assume $P(n)$ holds for some $n \in \mathbb{N}$, i.e. assume $x_n = \frac{(n+1)(2n+1)(2n+3)}{3}$. Then

$$\begin{aligned}
x_{n+1} &= x_n + (2(n+1)+1)^2 && \text{by recursive def. of } x_{n+1} \\
&= \frac{(n+1)(2n+1)(2n+3)}{3} + (2(n+1)+1)^2 && \text{by IH} \\
&= \frac{(n+1)(2n+1)(2n+3) + 3(2(n+1)+1)^2}{3} \\
&= \frac{(n+1)(2n+1)(2n+3) + 3(2n+3)^2}{3} \\
&= \frac{(2n+3)}{3}\left[(n+1)(2n+1) + 3(2n+3)\right] \\
&= \frac{(2n+3)}{3}\left[2n^2 + 3n + 1 + 6n + 9\right] \\
&= \frac{(2n+3)}{3}\left[2n^2 + 9n + 10\right] \\
&= \frac{(2n+3)}{3}\left[(2n+5)(n+2)\right] \\
&= \frac{(n+1+1)(2(n+1)+1)(2(n+1)+3)}{3}
\end{aligned}$$

Thus, $P(n+1)$ holds, which completes the proof of the induction step. □

Q5. [**4 points**] Determine whether each of the following statements is true for arbitrary sets A, B. If the statement is true, give an **indirect proof**. If the statement is false, give a **counterexample and explanation**. For your counterexample, give concrete sets A and B, (subsets of $\{1, 2, 3\}$ will suffice) and clearly explain how they show the statement can be false.

(a) If $A \times B = \emptyset$, then $A = \emptyset$ or $B = \emptyset$.

Solution: This statement is true.

Assume $A \neq \emptyset$ and $B \neq \emptyset$. Then $\exists a \in A$ and $\exists b \in B$. Therefore, $(a, b) \in A \times B$, hence $A \times B \neq \emptyset$.

(b) If $A - B = \emptyset$, then $B \subseteq A$.

Solution: This can be false. Counterexample: Let $A = \{1\}$ and $B = \{1, 2\}$. Then $A - B = \emptyset$ and $B \nsubseteq A$.

Q6. [**3 points**] Let S, T, W be arbitrary sets.

Give a rigorous proof to show that $(T \cup W) - S = (T - S) \cup (W - S)$.

Clearly justify each step! Be sure to use appropriate mathematical notation throughout.

Solution:

$$\begin{aligned}
x \in (T \cup W) - S &\iff x \in T \cup W \text{ and } x \notin S && \text{by def. of } - \\
&\iff \big(x \in T \text{ or } x \in W\big) \text{ and } x \notin S && \text{by def. of } \cup \\
&\iff \big(x \in T \text{ and } x \notin S\big) \text{ or } \big(x \in W \text{ and } x \notin S\big) \\
& \qquad\qquad \text{since } (P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R) \\
&\iff \big(x \in T - S\big) \text{ or } \big(x \in W - S\big) && \text{by def of } - \\
&\iff x \in \big(T - S\big) \cup \big(W - S\big) && \text{by def of } \cup
\end{aligned}$$

Therefore, $(T \cup W) - S = (T - S) \cup (W - S)$. □

Q7. **[6 points]** Let $\sim$ be a relation on $\mathbb{Z} \times \mathbb{Z}$ defined by the following rule:

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}, \quad (a, b) \sim (c, d) \iff a < c \text{ and } b < d.$$

For this question, you must use the formal definition of $<$ and the axiom related to $\mathbb{N}$ to justify your answers. You may also use the following proposition, seen in class:

Prop. If $a \in \mathbb{Z}$, then exactly one (one and only one) of the following statements is true:

$$a \in \mathbb{N} \quad \text{or} \quad a = 0 \quad \text{or} \quad -a \in \mathbb{N}.$$

You do not need to show all steps related to the first five axioms of $\mathbb{Z}$. For example, you can simplify $(a - b) + b = a$ without citing any axioms.

a) Is $\sim$ **reflexive**? If so, prove it; otherwise, give a counterexample and explanation.

Solution: $\sim$ is not reflexive. Counterexample: Take $(1, 2) \in \mathbb{Z} \times \mathbb{Z}$. Then $1 - 1 = 0 \notin \mathbb{N}$, so $1 \not< 1$. Therefore, $(1, 2) \nsim (1, 2)$.

(b) Is $\sim$ **symmetric**? If so, prove it; otherwise, give a counterexample and explanation.

Solution: No, $\sim$ is not symmetric. Counterexample: $(0, 0), (1, 1) \in \mathbb{Z} \times \mathbb{Z}$ since $0 < 1$ and $0 < 1$. But $(1, 1) \nsim (0, 0)$ since $0 - 1 = -1 \notin \mathbb{N}$.

(c) Is $\sim$ **transitive**? If so, prove it; otherwise, give a counterexample and explanation.

Solution: Yes, $\sim$ is transitive. Proof: Let $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z}$.

Assume $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$.

Then $a < c$ and $b < d$ and $c < e$ and $d < f$.

$$\begin{aligned}
&\implies c - a, d - b, e - c, f - d \in \mathbb{N} && \text{by def. of } < \\
&\implies (c - a) + (e - c) \in \mathbb{N} \text{ and } (d - b) + (f - d) \in \mathbb{N} && \text{since } \mathbb{N} \text{ is closed under } + \\
&\implies e - a \in \mathbb{N} \text{ and } f - b \in \mathbb{N} && \mathbb{Z} \text{ arithmetic} \\
&\implies a < e \text{ and } b < f && \text{def. of } < \\
&\implies (a, b) \sim (e, f) && \text{def. of } \sim.
\end{aligned}$$

Therefore, $\sim$ is transitive. □

Q8. **[5 points]**

(a) How many elements are there in $\mathbb{Z}_7$? List them all.

Solution: There are 7 elements given by $[0], [1], [2], [3], [4], [5], [6]$. Of course $[0] = [7]$ so $[1], [2], [3], [4], [5], [6], [7]$ is also a correct answer.

(b) Among the elements of $\mathbb{Z}_7$, find all $[x] \in \mathbb{Z}_7$ that satisfy $([x] \odot [x]) \oplus [x] = [2]$. Show all your work to justify your answer!

Solution: We compute $([x] \odot [x]) \oplus [x]$ for the 7 values of $[x] \in \mathbb{Z}_7$:

$[x]$	$[x] \odot [x]$	$([x] \odot [x]) \oplus [x]$
$[0]$	$[0]$	$[0]$
$[1]$	$[1]$	$[2]$
$[2]$	$[4]$	$[6]$
$[3]$	$[9] = [2]$	$[5]$
$[4]$	$[16] = [2]$	$[6]$
$[5]$	$[25] = [4]$	$[2]$
$[6]$	$[36] = [1]$	$[0]$

So the elements that satisfy $([x] \odot [x]) \oplus [x] = [2]$ are $[1]$ and $[5]$.

(c) Does $[10]$ have a multiplicative inverse in $\mathbb{Z}_7$? If so, find $[10]^{-1}$ and show that it is a multiplicative inverse. Your answer should be in terms of one of the canonical representatives.

Solution: Since $[10] \odot [5] = [15]$ and $[15] = [1]$ in $\mathbb{Z}_7$, we have $[10]^{-1} = [5]$.

Q9. **[6 points]** Consider the following subsets of real numbers:

$$A = \left\{ \frac{7n}{n+1} : n \in \mathbb{N} \right\} \qquad B = \left\{ 7 - \frac{6}{x} : x \in \mathbb{R}_{>0} \right\}$$

(a) Explain how and why the Completeness Axiom allows us to conclude that $\sup(A)$ exists.

Solution: The set A is nonempty since $\frac{7(1)}{1+1} \in A$.

Moreover, A is bounded above by 7 since, for all $n \in \mathbb{N}$, we have $\frac{7n}{n+1} < \frac{7n}{n} = 7$.

Since A is a nonempty subset of real numbers that is bounded above, the Completeness Axiom says that A must have a least upper bound. Thus, $\sup(A)$ exists.

(b) If it exists, find $\sup(B)$ and prove that it is a least upper bound for B. Otherwise, clearly justify why $\sup(B)$ does not exist.

Solution: We claim that $\sup(B) = 7$.

First, for all $x \in \mathbb{R}_{>0}$, we have $0 < \frac{6}{x}$. Thus, $7 - \frac{6}{x} < 7$. Thus, 7 is an upper bound for B.

Now, we claim that 7 is a least upper bound for B.

Suppose, to the contrary, that there is a smaller upper bound for B, say $\exists c \in \mathbb{R}$ such that $\forall b \in B, b \leq c < 7$.

$\implies \forall x \in \mathbb{R}_{>0}, \quad 7 - \frac{6}{x} \leq c < 7.$

$\implies \forall x \in \mathbb{R}_{>0}, \quad -\frac{6}{x} \leq c - 7 << 0.$

$\implies \forall x \in \mathbb{R}_{>0}, \quad \frac{6}{x} \geq 7 - c > 0.$

$\implies \forall x \in \mathbb{R}_{>0}, \quad \frac{6}{7-c} \geq x > 0.$

This shows that $\frac{6}{7-c}$ is an upper bound for $\mathbb{R}_{>0}$, which is a contradiction.

Therefore, no such c exists. We conclude that 7 is a least upper bound for B.

(c) Does $\min(A)$ exist? If so, find it and justify your answer. If not, fully justify your answer.

Solution: Yes, $\min(A) = \frac{7}{2}$. For all $n \in \mathbb{N}$, we have $\frac{7n}{n+1} \geq \frac{7n}{n+n} = \frac{7n}{2n} = \frac{7}{2}$. Thus, $\frac{7}{2}$ is a lower bound for A.

Using $n = 1$, we see that $\frac{7(1)}{1+1} = \frac{7}{2} \in A$.

Therefore, $\min(A) = \frac{7}{2}$ by definition.

(d) Does $\max(B)$ exist? If so, find it and justify your answer. If not, fully justify your answer.

Solution: Since $\sup(B)$ exists, if $\max(B)$ exists, then we'd have $\max(B) = \sup(B) = 7$. Since $7 - \frac{6}{x} < 7$, for all $x \in \mathbb{R}_{>0}$, it follows that $7 \notin B$. Thus, $\max(B)$ does not exist.

Q10. [7 points] Consider the functions below:

$$f : (\mathbb{R}_{>0} \times \mathbb{R}_{>0}) \to \mathbb{R}_{>0} \qquad f(x, y) = 5xy$$

$$g : \mathbb{R}_{>0} \to \mathbb{R}_{>0} \times \mathbb{R}_{>0} \qquad g(z) = \left(\tfrac{1}{5}, z\right)$$

(a) Is f injective? If so prove it; otherwise provide a concrete counterexample and briefly explain.

Solution: No, f is not injective. Counterexample: $(1, 2), (2, 1) \in \mathbb{R}_{>0} \times \mathbb{R}_{>0}$. $f(1, 2) = 5(1)(2) = 5(2)(1) = f(2, 1)$, but $(1, 2) \neq (2, 1)$.

(b) Is f surjective? If so prove it; otherwise provide a concrete counterexample and briefly explain.

Solution: Yes, f is surjective. Proof. Let $y \in \mathbb{R}_{>0}$. Then $\left(\frac{1}{5}, y\right) \in \mathbb{R}_{>0} \times \mathbb{R}_{>0}$ and we have $f\left(\frac{1}{5}, y\right) = 5\left(\frac{1}{5}\right)(y) = y$.

(c) Is g injective? If so prove it; otherwise provide a concrete counterexample and briefly explain.

Solution: Yes, g is injective. Let $z_1, z_2 \in \mathbb{R}_{>0}$.

$$\text{Assume } g(z_1) = g(z_2).$$
$$\text{Then } \left(\frac{1}{5}, z_1\right) = \left(\frac{1}{5}, z_2\right)$$
$$\implies \frac{1}{5} = \frac{1}{5} \text{ and } z_1 = z_2$$
$$\therefore z_1 = z_2.$$

□

(d) Is g surjective? If so prove it; otherwise provide a concrete counterexample and briefly explain.

Solution: No, g is not surjective. Counterexample: $(1, 1) \in \mathbb{R}_{>0} \times \mathbb{R}_{>0}$ but $g(z) = (1, 1) \iff (1/5, 1) = (1, 1)$ which is false. Thus, $\nexists z \in \mathbb{R}_{>0}$ such that $g(z) = (1, 1)$. □

(e) Is g a left inverse of f ? Justify your answer.

Solution: No, since f is not injective, f has no left inverse.

Alternatively, we can see that $g \circ f \neq \mathrm{id}_{\mathbb{R}_{>0} \times \mathbb{R}_{>0}}$, since, for example, $g \circ f(1, 1) = g(2) = \left(\frac{1}{5}, 2\right) \neq (1, 1)$.

(f) Is g a right inverse of f ? Justify your answer.

Solution: Yes! For all $z \in \mathbb{R}_{>0}$, we have

$$f \circ g(z) = f(g(z)) = f(\tfrac{1}{5}, z) = 5\left(\tfrac{1}{5}\right)(z) = z.$$

Thus, $f \circ g = \mathrm{id}_{\mathbb{R}_{>0}}$.

Q11. **[4 points]** Find $\lim_{n\to\infty} \frac{7n}{n+55}$.

Rigorously prove your answer using the formal definition of a limit.

Solution: We claim that $\lim_{n\to\infty} \frac{7n}{n+55} = 7$.

Note, for all $n \in \mathbb{N}$, we have

$$\left|\frac{7n}{n+55} - 7\right| = \left|\frac{7n}{n+55} - \frac{7(n+55)}{n+55}\right| = \left|\frac{-55}{n+55}\right| = \frac{55}{n+55} < \frac{55}{n}.$$

Let $\varepsilon > 0$.

Since $\mathbb{N}$ is not bounded above in $\mathbb{R}$, there exists $N \in \mathbb{N}$ such that $N > \frac{55}{\varepsilon}$. Consequently, $\frac{55}{N} < \varepsilon$.

Assume $n \geq N$. Then

$$\left|\frac{7n}{n+55} - 7\right| = \frac{55}{n+1} < \frac{55}{n} \leq \frac{55}{N} < \varepsilon.$$

Therefore, $\lim_{n\to\infty} \frac{7n}{n+55} = 7$, as claimed. □