MH1300 Foundations of Mathematics – Solutions

Final Examination, Academic Year 2015/2016, Semester 1

November 25, 2025

Summary

This paper assesses foundational proof techniques and discrete structures: quantifiers, number theory, induction, well-ordering, functions, equivalence relations, and set operations. The questions range from basic direct arguments and proof by cases to more conceptual reasoning about images of functions and equivalence class partitions. Core methods include direct proofs, proof by contradiction, proof by cases (via the Quotient–Remainder Theorem), mathematical induction, and element-chasing in sets and products. Several problems admit alternative viewpoints (e.g. algebraic manipulation, logical equivalences, or structural set identities), though standard textbook approaches are sufficient for full credit. Overall difficulty is moderate, with emphasis on clarity of logical structure and correct use of definitions.

Question 1 [10 marks]

Prove or disprove each of the following.

(a) $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \exists z \in \mathbb{R}, z^2 > x - y$. [5 marks]

(b) $\forall x \in \mathbb{Q}, \forall y \in \mathbb{Q}, x < y \implies (\exists z \in \mathbb{Q}, x < z < y)$. [5 marks]

Solution.

(a) **True.**

Proof: Take $x = 0$. For any arbitrary $y \in \mathbb{R}$, choose

$$z = \sqrt{|y|} + 1.$$

Then $z > \sqrt{|y|}$, and so $z^2 > |y|$ since both z and $\sqrt{|y|}$ are non-negative. Hence

$$z^2 > |y| \geq -y = 0 - y = x - y,$$

so $z^2 > x - y$. Therefore, the statement is true. □

(b) **True.**

Proof: Fix arbitrary $x, y \in \mathbb{Q}$ and assume $x < y$. We choose

$$z = \frac{x+y}{2}.$$

Then:

$$x = \frac{1}{2}x + \frac{1}{2}x < \frac{1}{2}x + \frac{1}{2}y = z < \frac{1}{2}y + \frac{1}{2}y = y.$$

So $x < z < y$. Since $x, y \in \mathbb{Q}$, their average $z = \frac{x+y}{2} \in \mathbb{Q}$. Therefore, between any two distinct rationals, there exists a rational number. □

Mark Scheme:

(a) Correctly identify the statement as true, choose a suitable x and z, and justify $z^2 > x-y$ with proper quantifier interpretation and inequalities. [5]

(b) Correctly state and prove existence of $z = \frac{x+y}{2}$ with $x < z < y$ and $z \in \mathbb{Q}$, explaining both the inequality chain and rationality. [5]

Question 2 [15 marks]

(a) Prove that if $a \in \mathbb{Z}$, then $a(a^2+2)$ is divisible by 3. [7 marks]

(b) Suppose that $q \in \mathbb{Z}$ and $q > 1$, and that for any integers a, b, q divides ab implies that q divides a or q divides b. Prove that q is prime. [8 marks]

Solution.

(a) **Proof by Cases:**

Fix $a \in \mathbb{Z}$. By the Quotient–Remainder Theorem (with divisor 3), a is of the form $3k$, $3k+1$, or $3k+2$ for some $k \in \mathbb{Z}$.

Case 1: $a = 3k$. Then:

$$a(a^2+2) = 3k(9k^2+2),$$

which is divisible by 3.

Case 2: $a = 3k+1$. Then:

$$a^2+2 = (3k+1)^2+2 = 9k^2+6k+1+2 = 9k^2+6k+3 = 3(3k^2+2k+1).$$

So $a(a^2+2)$ is divisible by 3.

Case 3: $a = 3k+2$. Then:

$$a^2+2 = (3k+2)^2+2 = 9k^2+12k+4+2 = 9k^2+12k+6 = 3(3k^2+4k+2).$$

So again $a(a^2+2)$ is divisible by 3.

In all three cases, $3 \mid a(a^2+2)$. Hence $a(a^2+2)$ is divisible by 3 for all $a \in \mathbb{Z}$. □

(b) **Proof:**

Let $q \in \mathbb{Z}$ with $q > 1$, and suppose that whenever $q \mid ab$ for $a, b \in \mathbb{Z}$, we have $q \mid a$ or $q \mid b$. Suppose, for contradiction, that q is not prime. Then we can write

$$q = ab$$

for some integers a, b with $1 < a < q$ and $1 < b < q$.

Clearly $q \mid ab$ (since $ab = q$). By assumption, this implies $q \mid a$ or $q \mid b$. But $|a| < q$ and $|b| < q$, so q cannot divide a nor b. This is a contradiction.

Therefore q must be prime. □

Mark Scheme:

(a) Correct use of the Quotient–Remainder Theorem modulo 3, clear separation into three cases, and correct algebra showing $3 \mid a(a^2+2)$ in each case. [7]

(b) Correct setup of the contrapositive/contradiction argument, factorisation $q = ab$ with $1 < a, b < q$, use of the given divisibility property, and explanation why this yields a contradiction unless q is prime. [8]

Question 3 [10 marks]

Prove by mathematical induction that for every positive integer n,

$$\sum_{k=1}^{n} \frac{k^2}{(2k-1)(2k+1)} = \frac{n(n+1)}{4n+2}.$$

Solution.

Let $P(n)$ denote the above statement.

Base case $P(1)$:

$$\text{LHS} = \frac{1^2}{(1)(3)} = \frac{1}{3}, \quad \text{RHS} = \frac{1 \cdot 2}{4+2} = \frac{2}{6} = \frac{1}{3}.$$

So $P(1)$ is true.

Inductive step: Assume $P(n)$ holds:

$$\sum_{k=1}^{n} \frac{k^2}{(2k-1)(2k+1)} = \frac{n(n+1)}{4n+2}.$$

For $P(n+1)$:

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{k^2}{(2k-1)(2k+1)} &= \sum_{k=1}^{n} \frac{k^2}{(2k-1)(2k+1)} + \frac{(n+1)^2}{(2n+1)(2n+3)} \\
&= \frac{n(n+1)}{4n+2} + \frac{(n+1)^2}{(2n+1)(2n+3)} \\
&= \frac{n(n+1)(2n+3) + 2(n+1)^2}{2(2n+1)(2n+3)} \\
&= \frac{(n+1)\big[n(2n+3) + 2(n+1)\big]}{2(2n+1)(2n+3)} \\
&= \frac{(n+1)(2n^2+5n+2)}{2(2n+1)(2n+3)} \\
&= \frac{(n+1)(2n+1)(n+2)}{2(2n+1)(2n+3)} \\
&= \frac{(n+1)(n+2)}{2(2n+3)} = \frac{(n+1)(n+2)}{4n+6}.
\end{aligned}$$

This is exactly the RHS of $P(n+1)$.

Thus $P(n)$ holds for $n = 1$, and $P(n) \Rightarrow P(n+1)$ for all $n \in \mathbb{N}$. Therefore, by mathematical induction,

$$\sum_{k=1}^{n} \frac{k^2}{(2k-1)(2k+1)} = \frac{n(n+1)}{4n+2}$$

holds for all $n \in \mathbb{N}$. $\square$

Mark Scheme:

(a) Correct statement and verification of the base case. [2]

(b) Proper formulation of the induction hypothesis and clear substitution into the $(n+1)$-sum. [4]

(c) Accurate algebraic manipulation to obtain the required closed form for $n+1$ and a clear concluding statement of induction. [4]

Question 4 [10 marks]

(a) Use the Well-ordering Principle to prove that for any real number $a > 0$ and any positive integer n, $a^n > 0$. [5 marks]

(b) Prove that if n is a positive integer then one of the numbers $n, n+3, n+6, n+9$ is a multiple of 4. [5 marks]

Solution.

(a) **Proof by Well-Ordering Principle:**

Suppose not. Then there exists a real number $a > 0$ and some positive integer n_0 such that $a^{n_0} \leq 0$.

Let

$$S = \{n \in \mathbb{Z} : n > 0 \text{ and } a^n \leq 0\}.$$

Then $S \neq \emptyset$ since $n_0 \in S$.

By the Well-Ordering Principle, S has a least element, say $m \in S$. Clearly $1 \notin S$ because $a^1 = a > 0$ by assumption, so $m > 1$.

Since $a^m \leq 0$ and $a > 0$, we have

$$a^{m-1} = \frac{a^m}{a} \leq 0.$$

As $m > 1$, we have $m - 1 > 0$, so $m - 1 \in S$. This contradicts m being the least element in S.

Therefore, $a^n > 0$ for all positive integers n. □

(b) **Proof by Cases:**

Fix a positive integer $n \geq 1$. By the Quotient–Remainder Theorem with divisor 4, n is of the form $4k$, $4k+1$, $4k+2$, or $4k+3$ for some $k \in \mathbb{Z}$.

Case 1: $n = 4k$. Then n is a multiple of 4.

Case 2: $n = 4k+1$. Then $n + 3 = 4k + 4 = 4(k+1)$ is a multiple of 4.

Case 3: $n = 4k+2$. Then $n + 6 = 4k + 8 = 4(k+2)$ is a multiple of 4.

Case 4: $n = 4k+3$. Then $n + 9 = 4k + 12 = 4(k+3)$ is a multiple of 4.

In all cases, one of $n, n+3, n+6, n+9$ is a multiple of 4. □

Mark Scheme:

(a) Correct construction of the set S, application of the Well-Ordering Principle, and derivation of the contradiction via $m - 1$. [5]

(b) Proper use of the Quotient–Remainder Theorem modulo 4 and correct identification of which of $n, n+3, n+6, n+9$ is divisible by 4 in each case. [5]

Question 5 [20 marks]

(a) Find non-empty sets A, B, C and functions $f_0 : A \to B$, $g_0 : B \to C$, $f_1 : A \to B$ and $g_1 : B \to C$ such that

(i) f_0 is onto but $g_0 \circ f_0$ is not onto. [4 marks]

(ii) $g_1 \circ f_1$ is 1-1 but g_1 is not 1-1. [4 marks]

Justify your answer.

(b) Let $h : (1, \infty) \to (1, \infty)$ be defined by $h(x) = \frac{x}{x-1}$. Is h 1-1? Is h onto? Justify your answer. [6 marks]

(c) Let $F : A \to B$. Prove that if $X \subseteq A$ and F is 1-1 then $F(A - X) = F(A) - F(X)$. [6 marks]

Solution.

(a) (i) Let $A = [0, 1]$, $B = [0, 1]$, $C = [0, 1]$. Take $f_0(x) = x$ (onto) and $g_0(x) = \frac{1}{2}x$. Then

$$(g_0 \circ f_0)(x) = g_0(f_0(x)) = g_0(x) = \frac{1}{2}x.$$

The function $g_0 \circ f_0$ is not onto because for $y = 1$, there is no $x \in [0, 1]$ such that $\frac{1}{2}x = 1$.

However, $f_0(x) = x$ is onto on $[0, 1] \to [0, 1]$.

(ii) Let $A = [0, 1]$, $B = [0, 1]$, $C = [0, 1]$. Take $f_1(x) = \frac{1}{2}x$ and $g_1(x) = \left|x - \frac{1}{2}\right|$. Then

$$(g_1 \circ f_1)(x) = g_1\left(\frac{1}{2}x\right) = \left|\frac{1}{2}x - \frac{1}{2}\right| = \frac{1}{2}|x - 1|.$$

For $x \in [0, 1]$, we have $x - 1 \leq 0$, so

$$(g_1 \circ f_1)(x) = \frac{1}{2}(1 - x),$$

which is a linear function with non-zero slope on $[0, 1]$ and hence is 1-1.

However, $g_1(x) = \left|x - \frac{1}{2}\right|$ is not 1-1 because $g_1(0) = \frac{1}{2} = g_1(1)$.

(b) **Analysis of** $h(x) = \frac{x}{x-1}$ on $(1, \infty)$:

Is h 1-1 (injective)? Yes.

Suppose $h(x) = h(y)$ for $x, y > 1$. Then:

$$\frac{x}{x-1} = \frac{y}{y-1}.$$

Assuming $x \neq 1$ and $y \neq 1$ (which is true since $x, y > 1$), cross-multiplying gives

$$x(y - 1) = y(x - 1) \implies xy - x = xy - y \implies -x = -y \implies x = y.$$

Thus h is injective.

Is h onto (surjective)? Yes.

Take arbitrary $y \in (1, \infty)$. We want $x \in (1, \infty)$ such that $h(x) = y$:

$$\frac{x}{x-1} = y.$$

Then

$$1 + \frac{1}{x-1} = y \quad \Longrightarrow \quad \frac{1}{x-1} = y - 1 \quad \Longrightarrow \quad x = 1 + \frac{1}{y-1}.$$

Since $y > 1$, we have $y - 1 > 0$, so $\frac{1}{y-1} > 0$ and hence $x = 1 + \frac{1}{y-1} > 1$. Thus $x \in (1, \infty)$ and $h(x) = y$.

Therefore, h is surjective onto $(1, \infty)$. Since h is both injective and surjective, it is bijective. □

(c) **Proof:**

We show both inclusions.

($\subseteq$) Let $y \in F(A - X)$. Then $y = F(x)$ for some $x \in A - X$. Thus $x \in A$ and $x \notin X$, so $F(x) \in F(A)$.

If we had $F(x) \in F(X)$, then there would exist $x' \in X$ such that $F(x') = F(x)$. Since $x \notin X$ and $x' \in X$, we must have $x \neq x'$, contradicting the assumption that F is 1-1. Hence $F(x) \notin F(X)$.

Therefore $F(x) \in F(A)$ but $F(x) \notin F(X)$, i.e. $F(x) \in F(A) - F(X)$. So

$$F(A - X) \subseteq F(A) - F(X).$$

($\supseteq$) Let $y \in F(A) - F(X)$. Then $y \in F(A)$, so there exists $x \in A$ such that $y = F(x)$.

If $x \in X$, then $y = F(x) \in F(X)$, which contradicts $y \notin F(X)$. Therefore $x \notin X$, so $x \in A - X$ and hence $y = F(x) \in F(A - X)$.

Thus $F(A) - F(X) \subseteq F(A - X)$.

Combining both inclusions, we conclude $F(A - X) = F(A) - F(X)$. □

Mark Scheme:

(a) Construction of valid examples for f_0, g_0 and f_1, g_1 satisfying the stated properties, with clear verification of (i) surjectivity/non-surjectivity and (ii) injectivity/non-injectivity. [8]

(b) Correct tests for injectivity and surjectivity of h, including solving $\frac{x}{x-1} = y$ and justifying the domain/range conditions. [6]

(c) Proof of both inclusions $F(A - X) \subseteq F(A) - F(X)$ and $F(A) - F(X) \subseteq F(A - X)$ using injectivity and the definitions of image and set difference. [6]

Question 6 [15 marks]

(a) Suppose that R and S are equivalence relations on a non-empty set A. Let $A/R = \{[a]_R \mid a \in A\}$ be the set of equivalence classes of R. Similarly $A/S = \{[a]_S \mid a \in A\}$ is the set of equivalence classes of S. Prove that if $A/R \subseteq A/S$, then $R = S$. [8 marks]

(b) Let T be a relation on the set of positive integers defined by $(a, b) \in T$ if and only if $\frac{a}{b} = 2^m$ for some $m \in \mathbb{Z}$. Prove that T is an equivalence relation. [7 marks]

Solution.

(a) **Proof:**

Assume $A/R \subseteq A/S$. Recall that A/R and A/S are both partitions of A into equivalence classes.

Step 1: $R \subseteq S$.

Let $(a, b) \in R$. Then a and b are R-equivalent, so they lie in the same R-equivalence class:

$$[a]_R = [b]_R \in A/R.$$

Since $A/R \subseteq A/S$, there exists some $c \in A$ such that

$$[a]_R = [c]_S.$$

Thus $a, b \in [c]_S$, and hence a and b are S-equivalent, i.e. $(a, b) \in S$. Therefore, $R \subseteq S$.

Step 2: $S \subseteq R$.

Let $(a, b) \in S$. Then a and b are S-equivalent, so

$$[a]_S = [b]_S.$$

Now A/R is a partition of A, so there is a unique R-equivalence class containing a, namely $[a]_R \in A/R$. By assumption $A/R \subseteq A/S$, so $[a]_R$ is also an S-equivalence class.

But $a \in [a]_R$ and $a \in [a]_S$. In a partition, different equivalence classes are disjoint. Hence the only way both $[a]_R$ and $[a]_S$ can contain a is if they are equal:

$$[a]_R = [a]_S.$$

Since $b \in [a]_S$, we also have $b \in [a]_R$, so a and b are R-equivalent, i.e. $(a, b) \in R$. Therefore $S \subseteq R$.

Combining both inclusions, we get $R = S$. $\square$

(b) **Showing T is an Equivalence Relation:**

We show that T is reflexive, symmetric, and transitive.

Reflexive: For any positive integer a, we have

$$\frac{a}{a} = 1 = 2^0$$

and $0 \in \mathbb{Z}$, so $(a, a) \in T$.

Symmetric: Suppose $(a, b) \in T$. Then $\frac{a}{b} = 2^m$ for some $m \in \mathbb{Z}$. Thus

$$\frac{b}{a} = \frac{1}{2^m} = 2^{-m}.$$

Since $-m \in \mathbb{Z}$, we have $(b, a) \in T$.

Transitive: Suppose $(a, b) \in T$ and $(b, c) \in T$. Then $\frac{a}{b} = 2^m$ and $\frac{b}{c} = 2^n$ for some $m, n \in \mathbb{Z}$. Hence

$$\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c} = 2^m \cdot 2^n = 2^{m+n},$$

and $m + n \in \mathbb{Z}$. Therefore $(a, c) \in T$.

Since T is reflexive, symmetric, and transitive, it is an equivalence relation. □

Mark Scheme:

(a) Correct use of equivalence classes and partitions to show $R \subseteq S$ and $S \subseteq R$, including the uniqueness/disjointness of classes argument. [8]

(b) Verification of reflexivity, symmetry, and transitivity for T using the representation $\frac{a}{b} = 2^m$ and closure of $\mathbb{Z}$ under addition and negation. [7]

Question 7 [20 marks]

(a) Prove that for any sets A and B, $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$. [5 marks]

(b) For any set A let $\mathcal{P}(A) = \{X \mid X \subseteq A\}$ be the power set of A. Are there sets A and B such that $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$? Justify your answer. [5 marks]

(c) Are the following true for any non-empty sets A, B, C and D? In each case, prove or give a counter-example.

(i) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$. [5 marks]

(ii) $(C \times C) - (A \times B) = (C - A) \times (C - B)$. [5 marks]

Solution.

(a) **Proof:**

We show the two sets are equal by double inclusion.

Let $x \in (A - B) \cup (B - A)$.

$\Leftrightarrow \quad x \in A - B \quad \text{or} \quad x \in B - A$

$\Leftrightarrow \quad (x \in A \text{ and } x \notin B) \quad \text{or} \quad (x \in B \text{ and } x \notin A)$ (by definition of set difference)

$\Leftrightarrow \quad (x \in A\text{or } x \in B) \quad \text{and} \quad (x \notin B \text{ or } x \notin A)$ (distributive law)

$\Leftrightarrow \quad x \in A \cup B \quad \text{and} \quad \neg(x \in A \text{ and } x \in B)$ (De Morgan's Law)

$\Leftrightarrow \quad x \in A \cup B \quad \text{and} \quad x \notin A \cap B$

$\Leftrightarrow \quad x \in (A \cup B) - (A \cap B)$.

Thus $(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B)$. The reverse inclusion can be shown by reversing the steps, so the sets are equal. □

(b) **No such sets exist.**

Justification: Suppose there are A, B such that $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$.

Note that $\emptyset \in \mathcal{P}(X)$ for any set X. In particular, $\emptyset \in \mathcal{P}(A - B)$.

However, since $\emptyset \in \mathcal{P}(A)$ and $\emptyset \in \mathcal{P}(B)$, we have $\emptyset \notin \mathcal{P}(A) - \mathcal{P}(B)$.

Therefore $\mathcal{P}(A - B) \neq \mathcal{P}(A) - \mathcal{P}(B)$ for any sets A and B, a contradiction. So no such sets exist. □

(c) (i) **False.**

Counterexample: Let $A = \{0\}$, $B = \{0\}$, $C = \{1\}$, $D = \{2\}$.

Then:

$$(A \times B) \cup (C \times D) = \{(0, 0)\} \cup \{(1, 2)\} = \{(0, 0), (1, 2)\}.$$

But:

$$(A \cup C) \times (B \cup D) = \{0, 1\} \times \{0, 2\} = \{(0, 0), (0, 2), (1, 0), (1, 2)\}.$$

These are not equal, so the statement is false.

(ii) **False.**
Counterexample: Let $C = B = \{0\}$ and $A = \{1\}$.
Then:

$$(C \times C) - (A \times B) = \{(0, 0)\} - \{(1, 0)\} = \{(0, 0)\},$$

but:

$$(C - A) \times (C - B) = \{0\} \times \emptyset = \emptyset.$$

These are not equal, so the statement is false.

Mark Scheme:

(a) Correct double-inclusion proof using membership logic, distributive laws, and De Morgan's laws to show equality of symmetric difference forms. [5]

(b) Clear explanation that $\emptyset$ belongs to $\mathcal{P}(A - B)$ but not to $\mathcal{P}(A) - \mathcal{P}(B)$, leading to impossibility for all A, B. [5]

(c) (i) Construction of concrete sets A, B, C, D and verification that the two sides of the equality give different Cartesian products. [5]

(c) (ii) Construction of suitable A, B, C and comparison of $(C \times C) - (A \times B)$ with $(C - A) \times (C - B)$, showing explicit inequality. [5]