UNIVERSITY OF BRISTOL

Examination for the Degree of B.Sc. and M.Sci. (Level C/4)

FOUNDATIONS AND PROOF SOLUTIONS

B=Bookwork, **S**=Seen, **P**=Partially seen, **U**=Unseen

Remarks made in square brackets [such as these] are not necessary for a complete solution.

Section A: Short Questions

A1. Recall that for $a, b \in \mathbb{R}$, $(a, b) = \{x \in \mathbb{R} : \ a \leq x \leq b \}$. Define

$$f : \left(\frac{5}{2}, \infty\right) \to \left(\frac{3}{2}, \infty\right)$$

by

$$f(x) = \frac{3x}{2x-5}.$$

(a) (2 marks) Show that f is injective.

(b) (2 marks) Show that f is surjective.

(c) (2+2 marks) Find a formula for f^{-1}, and demonstrate that $f \circ f^{-1}$ is the identity function on $\mathbb{R}$.

Solutions: (B)

(a) Suppose $x_1, x_2 \in \left(\frac{5}{2}, \infty\right)$ with $f(x_1) = f(x_2)$. Thus

$$\frac{3x_1}{2x_1-5} = \frac{3x_2}{2x_2-5}.$$

Hence $3x_1(2x_2 - 5) = 3x_2(2x_1 - 5)$, and subtracting $6x_1x_2$ from both sides of this equation we get $-15x_1 = -15x_2$. Hence $x_1 = x_2$, which means that f is injective.

(b) Take $y \in \left(\frac{3}{2}, \infty\right)$. [Scratch work: We want $x \in \left(\frac{5}{2}, \infty\right)$ so that $f(x) = y$, or equivalently, $3x = y(2x - 5)$. So we want $x = \frac{5y}{2y-3}$. (One can check that with $y > 3/2$, we get $x > 5/2$.)]

So take $x = \frac{5y}{2y-3}$. Thus

$$f(x) = \frac{3\frac{5y}{2y-3}}{2\frac{5y}{2y-3} - 5} = \frac{15y}{10y - 5(2y-3)} = \frac{15y}{15} = y.$$

Hence f is surjective.

(c) $f^{-1}(y) = \frac{5y}{2y-3}$. Then for any $y \in \left(\frac{3}{2}, \infty\right)$, we have

$$f \circ f^{-1}(y) = f(f^{-1}(y)) = f\left(\frac{5y}{2y-3}\right) = \frac{3\frac{5y}{2y-3}}{2\frac{5y}{2y-3} - 5} = \frac{15y}{10y - 5(2y-3)} = y.$$

A2. (a) (3 marks) Negate the following statement:

$$\forall \varepsilon > 0,\ \exists \delta > 0 \text{ so that } (|x - x_0| < \delta \implies |f(x) - f(x_0)| < \varepsilon).$$

(b) (5 marks) Let P, Q, R be propositions. Use a truth table to prove that

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R).$$

Solutions: (B)

(a) $\exists \varepsilon > 0$ so that $\forall \delta > 0$, $(|x - x_0| < \delta \wedge |f(x) - f(x_0)| \geq \varepsilon$.

(b)

P	Q	R	$(Q \wedge R)$	$[P \vee (Q \wedge R)]$	$(P \vee Q)$	$(P \vee R)$	$[(P \vee Q) \wedge (P \vee R)]$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Thus for any truth values of P, Q, R, the truth values of $P \vee (Q \wedge R)$ and of $(P \vee Q) \wedge (P \vee R)$ are the same, proving (b).

A3. (a) (3 marks) List all the elements in the set $\{1, 2\} \times \{a, b\}$.

(b) (3 marks) List all the partitions of the set $\{a, b, c\}$.

(c) (2 marks) Is $2 \equiv 10 \pmod 3$? Justify your answer.

Solutions: (B)

(a) $\{1, 2\} \times \{a, b\} = \{(1, a),\ (1, b),\ (2, a),\ (2b)\}$.

(b) The partitions of the set $\{a, b, c\}$ are:

$$\{\{a, b, c\}\},\ \{\{a, b\},\ \{c\}\},\ \{\{a, c\},\ \{b\}\},\ \{\{b, c\},\ \{a\}\},\ \{\{a\},\ \{b\},\ \{c\}\}.$$

(c) $2 - 10 = -8$, which is not divisible by 3. Hence $\neg[2 \equiv 10 \pmod 3]$.

A4. (a) (5 marks) Use Euclid's algorithm to find hcf$(87, 33)$, and integers s, t so that

$$87s + 33t = \text{hcf}(87, 33).$$

(b) (3 marks) Find $x \in \mathbb{Z}$ so that $0 \leq x < 11$ and $x \equiv 5^7 \pmod{11}$.

Solutions: (B)

(a) We have

$$\begin{aligned} 87 &= 2 \cdot 33 + 21 \\ 33 &= 1 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ [9 &= 3 \cdot 3 + 0] \end{aligned}$$

[So $3 = \text{hcf}(87, 33)$.] Thus

$$\begin{aligned} 3 &= 12 - 9 \\ &= 12 - (21 - 12) \\ &= 2 \cdot 12 - 21 \\ &= 2 \cdot (33 - 21) - 21 \\ &= 2 \cdot 33 - 3 \cdot 21 \\ &= 2 \cdot 33 - 3 \cdot (87 - 2 \cdot 33) \\ &= 8 \cdot 33 - 3 \cdot 87. \end{aligned}$$

[Thus we take $s = -3$ and $t = 8$.]

(b) We have $5^2 \equiv 25 \equiv 3 \pmod{11}$, so $5^4 \equiv 9 \equiv -2 \pmod{11}$. Thus $5^6 \equiv 3 \cdot (-2) \equiv -6 \equiv 5 \pmod{11}$, so $5^7 \equiv 25 \equiv 3 \pmod{11}$.

A5. (a) (3 marks) State the contrapositive of the following:

$$\exists N \in \mathbb{Z}_+ \text{ so that } n > N \implies a_n > 3.$$

(b) (2 marks) Which of the following is correct?

$$|\mathbb{Z}| < |\mathcal{P}(\mathbb{Z})|; \;\; |\mathbb{Z}| = |\mathcal{P}(\mathbb{Z})|; \;\; |\mathcal{P}(\mathbb{Z})| < |\mathbb{Z}|.$$

(Here $\mathcal{P}(\mathbb{Z})$ denotes the power set of $\mathbb{Z}$.)

(c) (3 marks) Which of the following sets are countable?

$$\mathbb{Z}; \;\; \mathbb{Q} \times \mathbb{Q}_+; \;\; \mathbb{R}.$$

Solutions: (B)

(a) $\exists N \in \mathbb{Z}_+$ so that $a_n \leq 3 \implies n \leq N$.

(b) $|\mathbb{Z}| < |\mathcal{P}(\mathbb{Z})|$.

(c) $\mathbb{Z}$ and $\mathbb{Q} \times \mathbb{Q}_+$ are countable.

Section B: Longer Questions

B1. (a) (6 marks) Let A, B be subsets of a set X. Prove that

$$(A \setminus B)^c = A^c \cup B.$$

(b) (5 marks) Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = |x^3|$. Let

$$V = \{x \in \mathbb{R} : \ 27 \leq x < \infty \}.$$

Find $f^{-1}(V)$.

(c) (5 marks) Suppose $g : X \to Y$ is sujective and $W \subseteq Y$. Show that $W \subseteq g(g^{-1}(W))$.

(d) (8 marks) Use induction on n to show that $\forall n \in \mathbb{Z}$ with $n \geq 2$,

$$\sum_{i=2}^{n} \frac{1}{(i-1)i} = 1 - \frac{1}{n}.$$

(e) (6 marks) Suppose $A, B_1, B_2, B_3, \ldots$ are subsets of a set X. Prove that for all $n \in \mathbb{Z}$ with $n \geq 1$, we have

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n).$$

Solutions:

(a) (S) Suppose $x \in X$. Thus:

$$\begin{aligned} x \in (A \setminus B)^c &\iff \neg(x \in A \setminus B) \\ &\iff \neg(x \in A \wedge x \notin B) \\ &\iff \neg(x \in A) \vee \neg(x \notin B) \\ &\iff (x \notin A) \vee (x \in B) \\ &\iff (x \in A^c) \vee (x \in B). \end{aligned}$$

Thus the elements of X that are in $(A \setminus B)^c$ are exactly the elements of X that are in $A^c \cup B$; hence $(A \setminus B)^c = A^c \cup B$.

(b) (P)

$$\begin{aligned} f^{-1}(V) &= \{x \in \mathbb{R} : \ f(x) \in V \} \\ &= \{x \in \mathbb{R} : \ |x^3| \in V \} \\ &= \{x \in \mathbb{R} : \ 27 \leq |x^3| < \infty \} \\ &= \{x \in \mathbb{R} : \ 3 \leq x < \infty \text{ or } -\infty < x \leq -3 \} \\ &= (\infty, -3] \cup [3, \infty). \end{aligned}$$

(c) (S) Take $y \in W$. Since g is surjective, there is some $x \in X$ so that $g(x) = y$. So $g(x) = y \in W$, which means that $x \in g^{-1}(W)$. Hence $y = g(x) \in g(g^{-1}(W))$. Hence $W \subseteq g(g^{-1}(W))$.

(d) (P) For $n \in \mathbb{Z}$ with $n \geq 2$, let $P(n)$ be the proposition

$$\sum_{i=2}^{n} \frac{1}{(i-1)i} = 1 - \frac{1}{n}.$$

[Base case] We have $\frac{1}{(2-1)2} = \frac{1}{2} = 1 - \frac{1}{2}$. Hence $P(1)$ holds.

[Induction step] Suppose $k \in \mathbb{Z}$ with $k \geq 2$ so that $P(k)$ holds. Then we have

$$\begin{aligned}\sum_{i=2}^{k+1} \frac{1}{(i-1)i} &= \frac{1}{(k+1-1)(k+1)} + \sum_{i=2}^{k} \frac{1}{(i-1)i} \\ &= \frac{1}{k(k+1)} + 1 - \frac{1}{k} \\ &= 1 + \frac{1-(k+1)}{k(k+1} \\ &= 1 - \frac{k}{k(k+1)} \\ &= 1 - \frac{1}{k+1}.\end{aligned}$$

Hence $P(k) \implies P(k+1)$, so by the Principle of Mathematical Inductions, we have that $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq 2$.

(e) (U) Let $S(n)$ be the proposition

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n).$$

We argue by induction on n. $S(1)$ holds, as this proposition states that $A \cup B_1 = A \cup B_1$. So suppose that $k \geq 1$ and that $S(k)$ holds. Set $B = B_1 \cap \cdots \cap B_k$. Suppose $x \in X$. Let P, Q, R be the propositions that $x \in A$, $x \in B$, $x \in B_{k+1}$. We have

$$\begin{aligned}x \in A \cup (B_1 \cap \cdots \cap B_{k+1}) &\iff x \in A \cup (B \cap B_{k+1}) \\ &\iff x \in A \vee (x \in B \cap B_{k+1}) \\ &\iff x \in A \vee (x \in B \wedge x \in B_{k+1}) \\ &\iff P \vee (Q \wedge R) \\ &\iff (P \vee Q) \wedge (P \vee R) \\ &\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in B_{k+1}) \\ &\iff (x \in A \cup B) \wedge (x \in A \cup B_{k+1}) \\ &\iff [x \in (A \cup B_1) \cap \cdots \cap (A \cup B_k)] \wedge (x \in A \cup B_{k+1}) \\ &\iff x \in (A \cup B_1) \cap \cdots \cap (A \cup B_k) \cap (A \cup B_{k+1}).\end{aligned}$$

Hence $S(k) \implies S(k+1)$, so $S(n)$ holds for all $n \in \mathbb{Z}_+$.

B2. (a) (9 marks) Find all primes p so that for some $n \in \mathbb{Z}_+$, $5p + 16 = n^2$. Justify your answer carefully.

(b) (4 marks) Define $f : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ by $f(m, n) = 2^m 3^n$. Show that f is injective.

(c) (4 marks) Suppose that $a, b, c \in \mathbb{Z}_+$ with $c = \text{hcf}(a, b)$. Take $x, y \in \mathbb{Z}_+$ so that $a = cx$, $b = cy$. Show that $\text{hcf}(x, y) = 1$. (Suggestion: Argue by contradiction.)

(d) (7 marks) Suppose that $f : X \to Y$ and $g : Y \to Z$ are bijective functions. Show that $g \circ f : X \to \mathbb{Z}$ is bijective.

(e) (6 marks) Suppose $f : X \to Y$ is bijective, and $A \subseteq X$ with A countable. Show that there is some $B \subseteq Y$ so that B is countable.

Solutions:

(a) (S) Suppose we have p prime so that $5p + 16 = n^2$ for some $n \in \mathbb{Z}_+$. Thus $5p = (n-4)(n+4)$, and so by the Fundamental Theorem of Arithmetic, we have either (1) $n - 4 = 1, n + 4 = 5p$, or (2) $n - 4 = 5, n + 4 = p$, or (3) $n - 4 = p, n + 4 = 5$, or (4) $n - 4 = 5p, n + 4 = 1$. Case (4) cannot occur as $n - 4 < n + 4$ and $5p > 1$.

Suppose $n - 4 = 1, n + 4 = 5p$. Thus $n = 5$, $5p = n + 4 = 9$, but 9 is not divisible by 5. So (again using the Fund. Thm. of Arith.), this case is impossible.

Suppose $n - 4 = 5, n + 4 = p$. Then $n = 9$ and $p = n + 4 = 13$. We know that 13 is prime, and that $5 \cdot 13 = 9^2$.

Suppose $n - 4 = p, n + 4 = 5$. Then $n = 1$, $p = n - 4 = -3$. But -3 is not a prime.

Hence the only solution is with $p = 13, n = 9$.

(b) (U) Suppose that $m, n, m', n' \in \mathbb{Z}_+$ so that $f(m, n) = f(m', n')$. Thus we have $2^m 3^n = 2^{m'} 3^{n'}$. By the Fundamental Theorem of Arithmetic, we must have $m = m'$ and $n = n'$. Hence $(m, n) = (m', n')$, meaning that f is injective.

(c) (P) Suppose, for the sake of contradiction, that $d = \text{hcf}(x, y) > 1$. Thus there are $u, v \in \mathbb{Z}_+$ so that $x = du$, $y = dv$. Then $a = cdu$, $b = cdv$, which means that cd is a common factor of a and b. But $cd > c$ [since $d > 1$], contradicting that c is the highest common factor of a and b.