Problem 1 (22 marks)

For $x, y \in \mathbb{Z}$ we define the set:

$$S_{x,y} = \{mx + ny : m, n \in \mathbb{Z}\}.$$

(a) Give five elements of $S_{4,-6}$. (5 marks)

(b) Give five elements of $S_{12,18}$. (5 marks)

For the following questions, let $d = \gcd(x, y)$ and z be the smallest positive number in $S_{x,y}$, or 0 if there are no positive numbers in $S_{x,y}$.

(c) (i) Show that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$. (4 marks)

(ii) Show that $d \leq z$. (2 marks)

(d) (i) Show that $z|x$ and $z|y$ (*Hint: consider* $(x \,\%\, z)$ *and* $(y \,\%\, z)$). (4 marks)

(ii) Show that $z \leq d$. (2 marks)

Remark

The result that there exists $m, n \in \mathbb{Z}$ such that $mx + ny = \gcd(x, y)$ is known as Bézout's Identity.

Solution

(a) We have:

$$\begin{array}{rlrlrl} -2 & = (1)4 + (1)(-6) & 6 & = (0)4 + (-1)(-6) & 0 & = (0)4 + (0)(-6) \\ 2 & = (-1)4 + (-1)(-6) & 4 & = (1)4 + (0)(-6) & & \ldots \end{array}$$

so

$$S_{4,-6} = \{\ldots, -2, 0, 2, 4, 6, \ldots\} = 2\mathbb{Z}$$

(b) We have:

$$\begin{array}{rlrlrl} -6 & = (1)12 + (-1)18 & 0 & = (0)12 + (0)18 & 6 & = (-1)12 + (1)18 \\ 12 & = (-2)12 + (2)18 & 18 & = (0)12 + (1)18 & & \ldots \end{array}$$

so

$$S_{12,16} = \{\ldots, -6, 0, 6, 12, 18, \ldots\} = 6\mathbb{Z}$$

(c) (i) $d|x$ and $d|y$, so $d|(mx + ny)$ for any integers m, n. Therefore, if $w \in S_{x,y}$, $d|w$. So $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$.

(ii) $z \in S_{x,y}$ so $d|z$, that is $z = kd$ for some integer k. If $z = 0$ then, as $\pm x, \pm y \in S_{x,y}$ it follows that $x = y = 0$ and hence $d = 0$. Otherwise $z > 0$, and as d is a non-negative integer, we have that $k \geq 0$. In both cases, $d \leq z$.

(d) (i) Let $r = (x \,\%\, z)$ and $q = (x \text{ div } z)$. From the definition of these operations, we have $x = qz + r$, or $r = x - qz$. Since $z \in S_{x,y}$, $z = mx + ny$ for some $m, n \in \mathbb{Z}$. Therefore, $r = (1 - m)x - ny$, so $r \in S_{x,y}$. From Q1(b), we have that $0 \leq r < z$. From the minimality of z, it follows that $r = 0$ and hence $z|x$. Similarly $z|y$.

(ii) The previous question shows that z is a common divisor of x and y. Therefore, by the definition of gcd, $z \leq d$.

Discussion

- For (a) and (b): 1 mark for each element correctly identified (justification not needed).
- Full marks for clear and correct proofs.
- Minor errors include missing logical steps in arguments
- Major errors include two+ minor errors; right proof "idea" but not clearly explained; or missing an inclusion when showing set equality.
- Good progress includes some logical argument

Problem 2 (12 marks)

For all $x, y \in \mathbb{Z}$ with $y > 1$:

(a) Prove that if $\gcd(x, y) = 1$ then there is at least one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$.
(*Hint: Use Bézout's identity*) (4 marks)

(b) Prove that if $\gcd(x, y) = 1$ and $y|kx$ then $y|k$. (4 marks)

(c) Prove that if $\gcd(x, y) = 1$ then there is at most one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$. (4 marks)

Solution

(a) Since $\gcd(x, y) = 1$, from Bézout's identity (or Q1), we have that there exists $m, n \in \mathbb{Z}$ such that $mx + ny = 1$. Let $w = m \,\%\, y$.

- From the lectures we have that $w \in [0, y)$.
- Also from the lectures we have that $m =_{(y)} w$, so:

$$\begin{array}{rcl} wx & =_{(y)} & mx \\ & = & mx + n \cdot 0 \\ & =_{(y)} & mx + ny \\ & = & 1 \end{array}$$

(b) Since $\gcd(x, y) = 1$, from (a) there exists w such that $wx =_{(y)} 1$. Since $y|kx$ we have $kx =_{(y)} 0$. Therefore:

$$\begin{array}{rcl} 0 & = & 0 \cdot w \\ & =_{(y)} & (kx)w \\ & = & k(wx) \\ & =_{(y)} & k \cdot 1 \\ & = & k \end{array}$$

So $y|k$ as required.

(c) Suppose $w, w' \in [0, y)$ are such that $wx =_{(y)} 1$ and $w'x =_{(y)} 1$. We will show that it must be the case that $w = w'$. Since $wx =_{(y)} w'x$, we have:

$$0 \quad =_{(y)} \quad wx - w'x \quad = \quad (w - w')x,$$

and therefore $y | (w - w')x$.

Since $\gcd(x, y) = 1$, from (b) we have that $y | (w - w')$, so $w - w' = ky$ for some $k \in \mathbb{Z}$.

As $w, w' \in [0, y)$ we have that:

- $w \geq 0$ and $w' < y$, so $w - w' > -y$, and therefore $k > -1$; and
- $w < y$ and $w' \geq 0$, so $w - w' < y$, and therefore $k < 1$.

So $k = 0$ and therefore $w = w'$.

Problem 3* (4 marks)

Prove that for all $m, n \in \mathbb{N}_{>0}$ with $n \leq m$:

$$\frac{3}{2}\big(n + (m \,\%\, n)\big) < m + n.$$

Solution

Suppose $x \geq \lfloor x \rfloor + 1$. Then $\lfloor x \rfloor + 1$ is an integer, smaller than x, but greater than $\lfloor x \rfloor$ – contradicting the definition of $\lfloor \cdot \rfloor$. Therefore $x < \lfloor x \rfloor + 1$.
Because $n \leq m$, we have $1 \leq \lfloor \frac{m}{n} \rfloor$, and from above we have $\frac{m}{n} < 1 + \lfloor \frac{m}{n} \rfloor$. Therefore,

$$m + n \quad = \quad n\big(\frac{m}{n} + 1\big) \quad < \quad n\big(\lfloor \frac{m}{n} \rfloor + 2\big) \quad \leq \quad 3n\lfloor \frac{m}{n} \rfloor.$$

Therefore,

$$3(m \,\%\, n) + 3n \;=\; 3m - 3n\lfloor \frac{m}{n} \rfloor + 3n \;=\; 2m + 2n + \big(m + n - 3n\lfloor \frac{m}{n} \rfloor\big) \;<\; 2m + 2n.$$

Therefore $\frac{3}{2}((m \,\%\, n) + n) < m + n$.

Discussion

- Minor errors include small logical errors or omissions
- Major errors include justifications based on non-standard definitions (e.g. using the "fractional" part) without references
- Shows progress includes working with a correct definition

Problem 4 (16 marks)

Use the laws of set operations (and any results proven in lectures) to prove the following identities:

(a) (Annihilation): $A \cap \emptyset = \emptyset$ (4 marks)

(b) $(A \setminus C^c) \cup (B \cap C) = C \cap (B \cup A)$ (4 marks)

(c) $A^c \oplus \mathcal{U} = A$ (4 marks)

(d) (De Morgan's law): $(A \cap B)^c = A^c \cup B^c$ (4 marks)

Proof assistant

https://www.cse.unsw.edu.au/~cs9020/cgi-bin/logic/21T3/set_theory/assignment

Solution

Here are some sample proofs (others exist):

(a)

$$\begin{aligned} A \cap \emptyset &= A \cap (A \cap A^c) && \text{(Complement with } \cap\text{)} \\ &= (A \cap A) \cap A^c && \text{(Associativity of } \cap\text{)} \\ &= A \cap A^c && \text{(Idempotence of } \cap\text{)} \\ &= \emptyset && \text{(Complement with } \cap\text{)} \end{aligned}$$

(b)

$$\begin{aligned} (A \setminus C^c) \cup (B \cap C) &= (A \cap C^{cc}) \cup (B \cap C) && \text{(Definition of } \setminus\text{)} \\ &= (A \cap C) \cup (B \cap C) && \text{(Double complement)} \\ &= (C \cap A) \cup (B \cap C) && \text{(Commutatitivity of } \cap\text{)} \\ &= (C \cap A) \cup (C \cap B) && \text{(Commutatitivity of } \cap\text{)} \\ &= (C \cap B) \cup (C \cap A) && \text{(Commutatitivity of } \cup\text{)} \\ &= C \cap (B \cup A) && \text{(Distributivity of } \cap \text{ over } \cup\text{)} \end{aligned}$$

(c)

$$\begin{aligned} A^c \oplus \mathcal{U} &= (A^c \cap \mathcal{U}^c) \cup (A^{cc} \cap \mathcal{U}) && \text{(Definition of } \oplus\text{)} \\ &= (A^c \cap (\mathcal{U}^c \cap \mathcal{U})) \cup (A^{cc} \cap \mathcal{U}) && \text{(Identity of } \cap\text{)} \\ &= (A^c \cap (\mathcal{U} \cap \mathcal{U}^c)) \cup (A^{cc} \cap \mathcal{U}) && \text{(Commutatitivity of } \cap\text{)} \\ &= (A^c \cap \emptyset) \cup (A^{cc} \cap \mathcal{U}) && \text{(Complement with } \cap\text{)} \\ &= (A^c \cap (A^c \cap A^{cc})) \cup (A^{cc} \cap \mathcal{U}) && \text{(Complement with } \cap\text{)} \\ &= ((A^c \cap A^c) \cap A^{cc}) \cup (A^{cc} \cap \mathcal{U}) && \text{(Associativity of } \cap\text{)} \\ &= (A^c \cap A^{cc}) \cup (A^{cc} \cap \mathcal{U}) && \text{(Idempotence of } \cap\text{)} \\ &= \emptyset \cup (A^{cc} \cap \mathcal{U}) && \text{(Complement with } \cap\text{)} \\ &= (A^{cc} \cap \mathcal{U}) \cup \emptyset && \text{(Commutatitivity of } \cup\text{)} \\ &= A^{cc} \cap \mathcal{U} && \text{(Identity of } \cup\text{)} \\ &= A^{cc} && \text{(Identity of } \cap\text{)} \\ &= A && \text{(Double complement)} \end{aligned}$$

$$
\begin{aligned}
A^c \oplus \mathcal{U} &= (A^c \cap \mathcal{U}^c) \cup (A^{cc} \cap \mathcal{U}) && \text{(Definition of } \oplus\text{)} \\
&= (A^c \cap (\mathcal{U}^c \cap \mathcal{U})) \cup (A^{cc} \cap \mathcal{U}) && \text{(Identity of } \cap\text{)} \\
&= (A^c \cap (\mathcal{U} \cap \mathcal{U}^c)) \cup (A^{cc} \cap \mathcal{U}) && \text{(Commutatitivity of } \cap\text{)} \\
&= (A^c \cap \emptyset) \cup (A^{cc} \cap \mathcal{U}) && \text{(Complement with } \cap\text{)} \\
&= (A^c \cap \emptyset) \cup (A \cap \mathcal{U}) && \text{(Double complement)} \\
&= (A^c \cap \emptyset) \cup A && \text{(Identity of } \cap\text{)} \\
&= A \cup (A^c \cap \emptyset) && \text{(Commutatitivity of } \cup\text{)} \\
&= (A \cup A^c) \cap (A \cup \emptyset) && \text{(Distributivity of } \cup \text{ over } \cap\text{)} \\
&= \mathcal{U} \cap (A \cup \emptyset) && \text{(Complement with } \cup\text{)} \\
&= (A \cup \emptyset) \cap \mathcal{U} && \text{(Commutatitivity of } \cap\text{)} \\
&= A \cup \emptyset && \text{(Identity of } \cap\text{)} \\
&= A && \text{(Identity of } \cup\text{)}
\end{aligned}
$$

(d) First, consider $(A \cap B) \cap (A^c \cup B^c)$:

$$
\begin{aligned}
(A \cap B) \cap (A^c \cup B^c) &= ((A \cap B) \cap A^c) \cup ((A \cap B) \cap B^c) && \text{(Distibutivity)} \\
&= (A \cap (B \cap A^c)) \cup (A \cap (B \cap B^c)) && \text{(Associativity)} \\
&= (A \cap (A^c \cap B)) \cup (A \cap (B \cap B^c)) && \text{(Commutativity)} \\
&= ((A \cap A^c) \cap B) \cup (A \cap (B \cap B^c)) && \text{(Associativity)} \\
&= (\emptyset \cap B) \cup (A \cap \emptyset) && \text{(Complement)} \\
&= (B \cap \emptyset) \cup (A \cap \emptyset) && \text{(Commutativity)} \\
&= \emptyset \cup \emptyset && \text{(Annihilation: (a))} \\
&= \emptyset && \text{(Identity).}
\end{aligned}
$$

From this it follows that $(A^c \cap B^c) \cap ((A^c)^c \cup (B^c)^c) = \emptyset$, so

$$
\begin{aligned}
\emptyset &= (A^c \cap B^c) \cap ((A^c)^c \cup (B^c)^c) \\
&= (A^c \cap B^c) \cap (A \cup B) && \text{(Double complement)} \\
&= (A \cup B) \cap (A^c \cap B^c) && \text{(Commutativity).}
\end{aligned}
$$

By the Principle of Duality, we therefore have:

$$(A \cap B) \cup (A^c \cup B^c) = \mathcal{U}.$$

By the uniqueness of complement it therefore follows that:

$$(A^c \cup B^c) = (A \cap B)^c$$

as required.

Discussion

- For top marks each rule should be on its own line, but multiple applications of the same rule on one line are ok.
- Minor errors include: one or two incorrect rule names (not counting multiple occurrences) ignoring small typos; one or two rule omissions (name or logical step – i.e. two rules on the same line). Double complementation is a commonly omitted rule.
- Major errors include: Two+ minor errors; omitting all rule names; unfinished proofs (e.g. finishing (c) at $(A * A^c) * (A * A^c)$)
- Good progress includes: One or two correct logical steps.

Problem 5 (12 marks)

Let $\Sigma = \{0, 1\}$. For each of the following, prove that the result holds for all sets $X, Y, Z \subseteq \Sigma^*$, or provide a counterexample to disprove:

(a) $(X \cap Y)^* = X^* \cap Y^*$ (4 marks)

(b) $(XY)^* = (YX)^*$ (4 marks)

(c) $X(Y \cap Z) = (XY) \cap (XZ)$ (4 marks)

Solution

(a) This is false. Consider $X = \{00\}$ and $Y = \{000\}$. Then

$$000000 \in X^* \text{ and } 000000 \in Y^* \text{ but } X \cap Y = \emptyset \text{ so } 000000 \notin (X \cap Y)^*.$$

(b) This is false. Consider $X = \{0\}$ and $Y = \{1\}$. Then $01 \in (XY)^*$ and $01 \notin (YX)^*$.

(c) This is false. Consider $X = \{0, 00\}$, $Y = \{0\}$, and $Z = \{00\}$. Then $Y \cap Z = \emptyset$ so $X(Y \cap Z) = \emptyset$; but $000 \in XY$ and $000 \in XZ$, so $000 \in (XY \cap XZ)$

Discussion

- Concrete examples for all answers are required for full marks.
- Minor errors for small logical omissions (e.g. not showing that the counterexamples work)
- Major errors include not giving a concrete counterexample for false answers
- Shows progress includes identifying if the statement is true/false without justification.

Problem 6 (12 marks)

(a) List all possible functions $f : \{a, b, c\} \to \{0, 1\}$, that is, all elements of $\{0, 1\}^{\{a,b,c\}}$. (4 marks)

(b) Describe a connection between your answer for (a) and $\text{Pow}(\{a, b, c\})$. (4 marks)

(c) Describe a connection between your answer for (a) and $\{w \in \{0,1\}^* : \text{length}(w) = 3\}$. (4 marks)

Solution

(a) There are eight functions from $\{a,b,c\}$ to $\{0,1\}$:

- f_0: $a \mapsto 0$, $b \mapsto 0$, $c \mapsto 0$
- f_1: $a \mapsto 0$, $b \mapsto 0$, $c \mapsto 1$
- f_2: $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 0$
- f_3: $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 1$
- f_4: $a \mapsto 1$, $b \mapsto 0$, $c \mapsto 0$
- f_5: $a \mapsto 1$, $b \mapsto 0$, $c \mapsto 1$
- f_6: $a \mapsto 1$, $b \mapsto 1$, $c \mapsto 0$
- f_7: $a \mapsto 1$, $b \mapsto 1$, $c \mapsto 1$

(b) We observe that the cardinality of $\text{Pow}(\{a,b,c\})$ is equal to the number of functions from $\{a,b,c\}$ to $\{0,1\}$. Indeed, for each function $f : \{a,b,c\} \to \{0,1\}$ we can associate a unique element of $\text{Pow}(\{a,b,c\})$ given by $f^{\leftarrow}(1)$. For example, f_0 corresponds to $\emptyset$; f_5 corresponds to $\{a,c\}$.

(c) We again observe that the cardinaltiy of $\Sigma^{=3}$ (where $\Sigma = \{0,1\}$) is equal to the number of functions from $\{a,b,c\}$ to $\{0,1\}$. Indeed, for each function $f : \{a,b,c\} \to \{0,1\}$ we can associate a unique element of $\Sigma^{=3}$ given by $f(a)f(b)f(c)$. For example f_0 corresponds to 000; f_5 corresponds to 101.

Discussion

- For full marks, functions should be clearly defined; the full connection between the sets should be identified; each numeric answer should have a small justification
- Minor errors include small typos that do induce an incorrect answer (e.g. doubling up on a function)
- Major errors include unclear function definitions; only matching cardinalities; numeric answers without justification; incorrect numeric answers with small justification
- Shows promise includes: one or more functions defined; well-founded incorrect numeric answers (e.g. m^2) without justification.

Problem 7* (6 marks)

Show that for any sets A, B, C there is a bijection between $A^{(B\times C)}$ and $(A^B)^C$.

Solution

$A^{(B\times C)}$ is the set of functions from $B \times C$ to A; and $(A^B)^C$ is the set of functions from C to X where X is the set of functions from B to A. For each $f \in A^{(B\times C)}$, and $c \in C$ let $g_{f,c} \in X$ denote the function from B to A defined as $g_{f,c}(b) = f(b,c)$. For each $f \in A^{(B\times C)}$, let $h_f \in X^C$ denote the function from C to X defined as $h_f(c) = g_{f,c}$. We claim that the map that takes f to h_f is a bijection.

Injection. First we show that the map is an injection. Take $f, f' \in A^{(B\times C)}$ with $f \neq f'$. Since $f \neq f'$ there exists $b \in B, c \in C$ such that $f(b,c) \neq f'(b,c)$. Therefore $g_{f,c}(b) \neq g_{f',c}(b)$ so $g_{f,c} \neq g_{f',c}$. But then $h_f(c) \neq h_{f'}(c)$ so $h_f \neq h_{f'}$. Therefore the map is injective.

Surjection. Consider any $h : C \to X$. Define $f_h : B \times C \to A$ by setting $f_h(b,c) = [h(c)](b)$. For any $c' \in C$ we have $g_{f_h,c} : B \to A$ is the function that maps b to $f_h(b,c) = [h(c)](b)$. That is, $g_{f_h,c} = h(c)$. But then h_{f_h} is the function that maps c to $g_{f_h,c} = h(c)$. That is $h_{f_h} = h$. Therefore the map is surjective.

Discussion

- For full marks, the argument should apply to any sets A, B, C, not just finite sets (i.e. cardinality arguments will generally not be sufficient).
- Minor errors include well-argued (i.e. defining a bijection) proof for finite sets
- Major errors include a cardinality-based argument that uses exponentiation properties
- Shows promise includes identifying the sets $A^{(B\times C)}$ and $(A^B)^C$.

Problem 8 (16 marks)

Recall the relation composition operator ; defined as:

$$R_1; R_2 = \{(a,c) : \text{there is a } b \text{ with } (a,b) \in R_1 \text{ and } (b,c) \in R_2\}$$

Let S be an arbitrary set. For each of the following, prove it holds for any binary relations $R_1, R_2, R_3 \subseteq S \times S$, or give a counterexample to disprove:

(a) $(R_1; R_2); R_3 = R_1; (R_2; R_3)$ (4 marks)

(b) $I; R_1 = R_1; I = R_1$ where $I = \{(x,x) : x \in S\}$ (4 marks)

(c) $(R_1 \cup R_2); R_3 = (R_1; R_3) \cup (R_2; R_3)$ (4 marks)

(d) $R_1; (R_2 \cap R_3) = (R_1; R_2) \cap (R_1; R_3)$ (4 marks)

Solution

(a) This is true. We have:

$$\begin{array}{lll} (a,d) \in (R_1;R_2);R_3 & \text{iff} & \text{there exists } c \in S \text{ such that } (a,c) \in R_1;R_2 \text{ and } (c,d) \in R_3 \\ & \text{iff} & \text{there exists } b,c \in S \text{ such that } (a,b) \in R_1 \text{ and } (b,c) \in R_2 \text{ and } (c,d) \in R_3 \\ & \text{iff} & \text{there exists } b \in S \text{ such that } (a,b) \in R_1 \text{ and } (b,d) \in R_2;R_3 \\ & \text{iff} & (a,d) \in R_1;(R_2;R_3) \end{array}$$

(b) This is true. Suppose $(a,b) \in R$. Then, because $(a,a) \in I$ we have $(a,b) \in I; R$. Also, because $(b,b) \in I$ we have $(a,b) \in R; I$.

Now suppose $(a, b) \in I; R$. Then there exists $c \in S$ such that $(a, c) \in I$ and $(c, b) \in R$. But from the definition of I, the only such c is $c = a$, so $(a, b) \in R$.

Finally suppose $(a, b) \in R; I$. Then there exists $c \in S$ such that $(a, c) \in R$ and $(c, b) \in I$. Again, from the definition of I, the only such c is $c = b$, so $(a, b) \in R$.

(c) This is true.

(d) This is false. Consider $R_1 = \{(1,2), (1,3)\}$, $R_2 = \{(2,4)\}$ and $R_3 = \{3,4\}$. Then we hae $R_2 \cap R_3 = \emptyset$, so $R_1; (R_2 \cap R_3) = \emptyset$. On the other hand, $(1,4) \in R_1 : R_2$ and $(1,4) \in R_1; R_3$, so $(R_1; R_2) \cap (R_1; R_3)$ is non-empty.

Discussion

For each question:

- Minor errors for small logical omissions (e.g. not showing that the counterexamples work)
- Major errors include only showing one "direction" of the equality (but correctly stating whether the statement is true/false); not giving a concrete counterexample (i.e. justification for false has ambiguity)
- Shows progress includes identifying if the statement is true/false without justification.