

MAT 1348 - Homework #3
- Solutions -

① $n \in \mathbb{Z}$. Prove that $3 \mid n^3 - n$.

The remainder of n after division by 3 can be 0 or 1 or 2.
Hence, we consider three cases:

case 1: n gives remainder 0 after division by 3,

i.e. n is divisible by 3

i.e. $n = 3k$ for some integer $k \in \mathbb{Z}$

$$\begin{aligned} \text{Then } n^3 - n &= n(n^2 - 1) = 3k(9k^2 - 1) \\ &= 3[k(9k^2 - 1)] = 3l, \end{aligned}$$

where $l = k(9k^2 - 1)$ is an integer as product of integers.

$$\therefore 3 \mid n^3 - n$$

case 2: n gives remainder 1 after division by 3,

i.e. $n = 3k + 1$ for some $k \in \mathbb{Z}$

$$\begin{aligned} \text{Then } n^3 - n &= n(n^2 - 1) = n(n-1)(n+1) = \\ &= (3k+1)3k(3k+2) \\ &= 3[(3k+1)k(3k+2)] = 3l, \end{aligned}$$

where $l = (3k+1)k(3k+2)$ is an integer.

$$\therefore 3 \mid n^3 - n$$

case 3: n gives remainder 2 after division by 3,

i.e. $n = 3k + 2$ for some $k \in \mathbb{Z}$

$$\begin{aligned} \text{Then } n^3 - n &= n(n^2 - 1) = n(n-1)(n+1) = \\ &= (3k+2)(3k+1)(3k+3) = \\ &= (3k+2)(3k+1)3(k+1) = \\ &= 3[(3k+2)(3k+1)(k+1)] = 3l, \end{aligned}$$

where $l = (3k+2)(3k+1)(k+1) \in \mathbb{Z}$.

$$\therefore 3 \mid n^3 - n.$$

The statement

p : "n is an integer." is equivalent to $p_1 \vee p_2 \vee p_3$ where

p_1 : "n = 3k for some $k \in \mathbb{Z}$ "

p_2 : "n = 3k + 1 for some $k \in \mathbb{Z}$ "

p_3 : "n = 3k + 2 for some $k \in \mathbb{Z}$ "

Also, we proved that if

q : "3 divides $n^3 - n$ ", then

$p_1 \rightarrow q$ and $p_2 \rightarrow q$ and $p_3 \rightarrow q$ are true.

Hence $p \rightarrow q \equiv (p_1 \vee p_2 \vee p_3) \rightarrow q$
 $\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q)$

is true.

2. (a) $(A - (B - C)) \cup (C - A) = C \cup (A - B)$

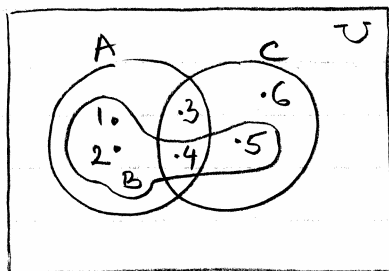
We will use the identity $X - Y = X \cap \bar{Y}$

$$\begin{aligned} & (A - (B - C)) \cup (C - A) = \\ & = (A \cap \overline{(B - C)}) \cup (C \cap \bar{A}) = \\ & = (A \cap \overline{(B \cap \bar{C})}) \cup (C \cap \bar{A}) = \\ & = (A \cap (\bar{B} \cup \bar{\bar{C}})) \cup (C \cap \bar{A}) \\ & = (A \cap (\bar{B} \cup C)) \cup (C \cap \bar{A}) \\ & = ((A \cap \bar{B}) \cup (A \cap C)) \cup (C \cap \bar{A}) \\ & = (A \cap \bar{B}) \cup ((A \cap C) \cup (C \cap \bar{A})) \\ & = (A \cap \bar{B}) \cup ((C \cap A) \cup (C \cap \bar{A})) \\ & = (A \cap \bar{B}) \cup (C \cap (A \cup \bar{A})) \\ & = (A \cap \bar{B}) \cup (C \cap U) \\ & = (A \cap \bar{B}) \cup C \\ & = C \cup (A \cap \bar{B}) \\ & = C \cup (A - B) \end{aligned}$$

De Morgan's Law
Complementation Law
Distribution
Associativity
Commutativity
Distributivity
Complement Law
Identity Law
Commutativity

(2b.) (i) If $A - C = B - C$, then $A = B$.

Consider



Let $U = \{1, 2, 3, 4, 5, 6\}$ be the universal set.
Let $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 4, 5\}$, $C = \{3, 4, 5, 6\}$.
Then $A - C = \{1, 2\}$
 $B - C = \{1, 2\}$
Hence, $A - C = B - C$ but $A \neq B$.

(ii) $f: A \rightarrow B$, $S, T \subseteq B$.
 $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$

We will prove two inclusions:

case 1: $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}(T)$

case 2: $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$

case 1: To prove that $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}(T)$,
let $x \in f^{-1}(S \cup T)$. Then

$f(x) \in S \cup T$ so $(f(x) \in S \text{ or } f(x) \in T)$.

If $f(x) \in S$, then $x \in f^{-1}(S)$.

Similarly, if $f(x) \in T$, then $x \in f^{-1}(T)$.

Therefore,

$(f(x) \in S \text{ or } f(x) \in T)$ implies that
 $(x \in f^{-1}(S) \text{ or } x \in f^{-1}(T))$, so $x \in f^{-1}(S) \cup f^{-1}(T)$.

Hence, for every $x \in f^{-1}(S \cup T)$, $x \in f^{-1}(S) \cup f^{-1}(T)$,
i.e. $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}(T)$.

case 2: To prove that $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$,
 let $x \in f^{-1}(S) \cup f^{-1}(T)$. Then
 $(x \in f^{-1}(S) \text{ or } x \in f^{-1}(T))$ so
 $(f(x) \in S \text{ or } f(x) \in T) \equiv f(x) \in S \cup T$
 Since $f(x) \in S \cup T$, $x \in f^{-1}(S \cup T)$.

Hence, if $x \in f^{-1}(S) \cup f^{-1}(T)$, then $x \in f^{-1}(S \cup T)$,
 i.e. $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$.

Since $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}(T)$ and
 $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$,
 we conclude that
 $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$.

3 i. $f: \mathbb{Z}_x \times \mathbb{Z}_y \rightarrow \mathbb{Z}_w$ $f(x, y) = -2x - y$

a) f is NOT one-to-one because

$$f(1, 0) = -2 \cdot 1 - 0 = -2 \quad \text{and}$$

$$f(2, 2) = -2 \cdot 2 - (-2) = -2$$

} any counter-example is a valid proof

(b) f is onto. Indeed, for any $w \in \mathbb{Z}$, let $x=0$ and $y=-w$
 Then $f(x, y) = f(0, -w) = -2 \cdot 0 - (-w) = w$

3 ii $g: \mathbb{Z}_x \times \mathbb{Z}_y \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ $g(x, y) = (x+y, -x)$ is a bijection
 $g^{-1}(a, b) = ?$

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. We want to find $(x, y) \in \mathbb{Z} \times \mathbb{Z}$
 such that $f(x, y) = (a, b)$
 $(x+y, -x) = (a, b)$

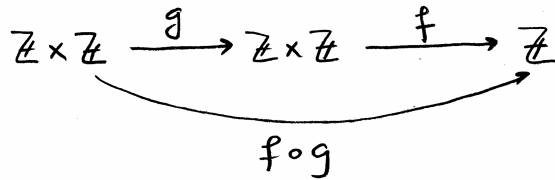
i.e. $x+y = a$

$-x = b \Rightarrow x = -b$ and

$y = a - x = a - (-b) = (a+b)$

Hence, $g^{-1}(a, b) = (-b, a+b)$.

(3iii)



Hence $f \circ g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$.

$$\begin{aligned} (f \circ g)(x, y) &= f(g(x, y)) = f(x+y, -x) \\ &= -2(x+y) - (-x) = \\ &= -x - 2y \end{aligned}$$

$f \circ g$ is NOT one-to-one. Indeed

$$f \circ g(0, 0) = -0 - 2 \cdot 0 = 0$$

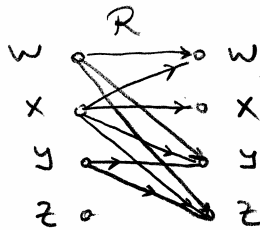
$$f \circ g(2, -1) = -2 - 2 \cdot (-1) = 0$$

} any counter-example proves the claim

$f \circ g$ is onto. Indeed, let $w \in \mathbb{Z}$, let $x = -w, y = 0$.

$$\text{Then } f \circ g(x, y) = f \circ g(-w, 0) = -(-w) - 2 \cdot 0 = w$$

(4)



R is NOT reflexive since $(z, z) \notin R$

R is NOT symmetric since $(w, y) \in R$ but $(y, w) \notin R$

[Other possibilities which prove that R is not symmetric:

- $(w, z) \in R$ but $(z, w) \notin R$
- $(x, y) \in R$ but $(y, x) \notin R$
- $(x, z) \in R$ but $(z, x) \notin R$
- $(y, z) \in R$ but $(z, y) \notin R$
- $(x, w) \in R$ but $(w, x) \notin R$]

R is antisymmetric. Indeed, for any $a, b \in \{w, x, y, z\}$, $a \neq b$, if $(a, b) \in R$, then $(b, a) \notin R$.

R is transitive. To prove this, we will check all possibilities:

Note that if $a, b \in \{w, x, y, z\}$, then
 (if $(a, a) \in R$ and $(a, b) \in R$, then $(a, b) \in R$) is true
 and (if $(a, b) \in R$ and $(b, b) \in R$, then $(a, b) \in R$) is true.
 Other possibilities are:

$$\begin{array}{l} ((w, y) \in R \text{ and } (y, z) \in R) \rightarrow (w, z) \in R \quad T \\ ((x, y) \in R \text{ and } (y, z) \in R) \rightarrow (x, z) \in R \quad T \\ ((x, w) \in R \text{ and } (w, y) \in R) \rightarrow (x, y) \in R \quad T \\ ((x, w) \in R \text{ and } (w, z) \in R) \rightarrow (x, z) \in R \quad T \end{array}$$

$$(5) (x_1, y_1) R (x_2, y_2) \iff x_1(1-y_2) = x_2(1-y_1)$$

• R is reflexive:

$$(x_1, y_1) R (x_1, y_1) \iff x_1(1-y_1) = x_1(1-y_1)$$

• R is symmetric:

If $(x_1, y_1) R (x_2, y_2)$, then $x_1(1-y_2) = x_2(1-y_1)$
 Then $x_2(1-y_1) = x_1(1-y_2)$, so $(x_2, y_2) R (x_1, y_1)$

• R is transitive:

Assume that $(x_1, y_1) R (x_2, y_2)$ and $(x_2, y_2) R (x_3, y_3)$.

$$\text{Then } x_1(1-y_2) = x_2(1-y_1) \quad (1)$$

$$\text{and } x_2(1-y_3) = x_3(1-y_2) \quad (2)$$

Note that R is a relation on $(\mathbb{R} - \{0\}) \times \mathbb{R}$, so

$x_1 \neq 0$ and $x_2 \neq 0$. Therefore,

$$\text{from (1): } 1-y_2 = \frac{x_2(1-y_1)}{x_1}, \text{ substitute it in (2)}$$

$$\text{to get } x_2(1-y_3) = x_3 \frac{x_2(1-y_1)}{x_1}. \text{ Now since } x_2 \neq 0,$$

$$(1-y_3) = x_3 \frac{1-y_1}{x_1}$$

$$x_1(1-y_3) = x_3(1-y_1), \text{ so } (x_1, y_1) R (x_3, y_3).$$