# OK, Beamer.

Rishabh Singh

April 2020

# P-Set 1 Question 2

## Q2

Show that

$$A = \{x \in \mathbb{R} \mid \cos x = 1\}$$

is a subset of

$$B = \{x \in \mathbb{R} \mid \sin x = 0\}.$$

**Proof.** Let's say $x \in A$. To prove $A \subseteq B$, we need to prove $x \in B$. Since $x \in A$, $\cos x = 1$. It is known that

$$\cos^2 x + \sin^2 x = 1$$

This means that

$$\begin{aligned} \sin x &= \sqrt{1 - \cos^2 x} \\ &= \sqrt{1 - 1} \\ &= 0 \end{aligned}$$

This means that $x \in B$, which means $A \subseteq B$.

# P-Set 1 Question 2

## Q2, continued

Show that

$$A = \{x \in \mathbb{R} \mid \cos x = 1\}$$

is a subset of

$$B = \{x \in \mathbb{R} \mid \sin x = 0\}.$$

Is $A$ a proper subset of $B$? Give reasons.

**Proof.** $A \subset B$ if $A \neq B$. We need to prove that $B \not\subseteq A$. We can prove this by providing a counter-example. Let $x \in B$.

$$sin^2 x + \cos^2 x = 1$$

$$cosx = \sqrt{1 - \sin^2}$$

$$= \pm 1$$

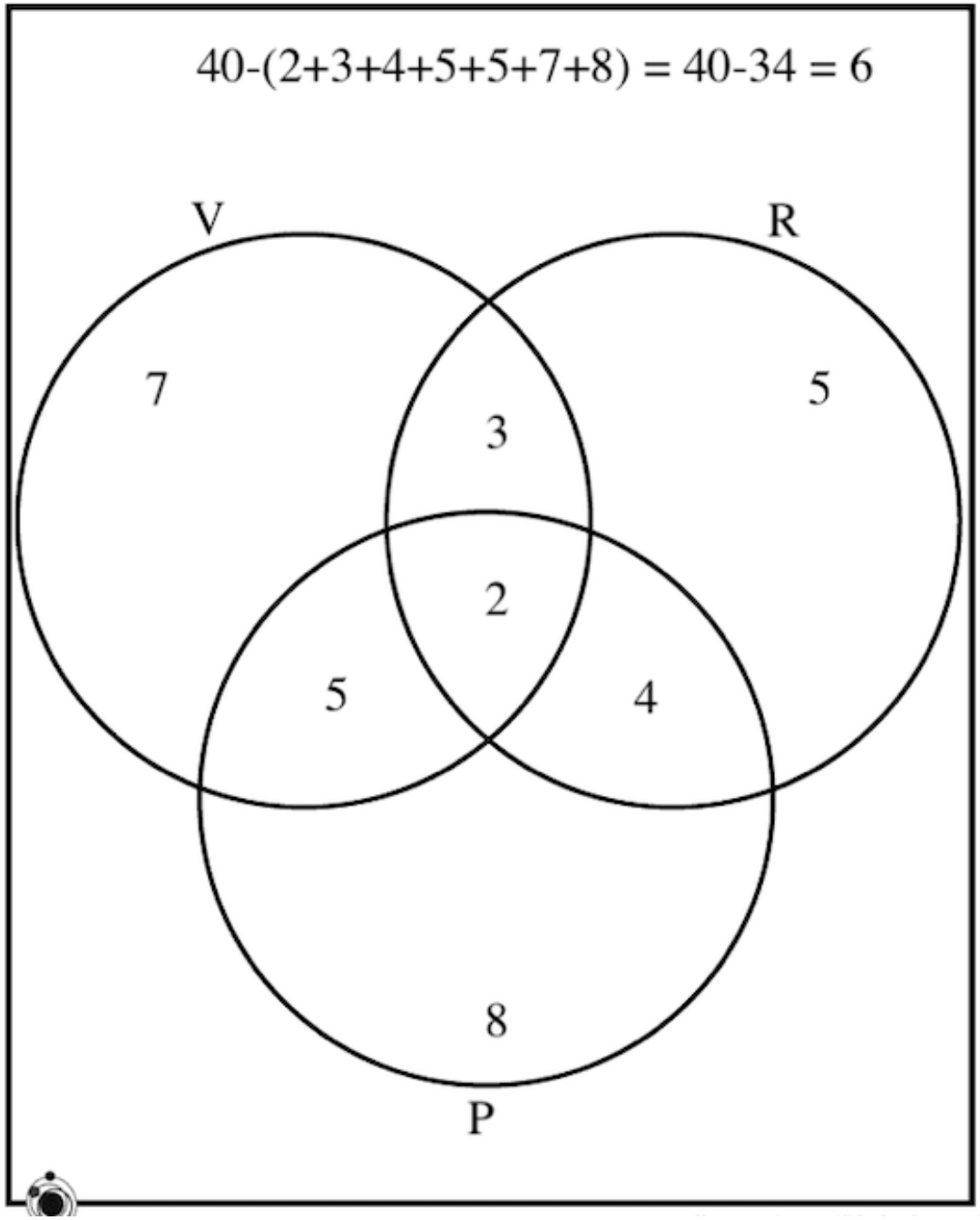
Since $\cos x = -1, x \notin A$, A is a proper subset of B.

# P-Set 1 Question 11

## Q11

In a class of 40 people studying music: 2 play violin, piano and recorder, 7 play at least violin and piano, 6 play at least piano and recorder, 5 play at least recorder and violin, 17 play at least violin, 19 play at least piano, and 14 play at least recorder. How many play none of these instruments?

# Answer



# P-Set 1 Question 13

## Q13

Let $A$ and $B$ be general sets. Determine the containment relation ($\subseteq$, $=$, none) that holds between

a) $\mathcal{P}(A \cup B)$ and $\mathcal{P}(A) \cup \mathcal{P}(B)$

**Proof.** Let $x \in \mathcal{P}(A) \cup \mathcal{P}(B)$. This means that $x \subseteq A$ or $x \subseteq B$. This means that $x \subseteq A \cup B$, which implies $x \in \mathcal{P}(A \cup B)$. This directly implies that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

However, this doesn't apply the other way around. If $x \subseteq A \cup B$, that doesn't mean $x \subseteq A$ or $x \subseteq B$. (Take $A = \{1, 2\}$, $B = \{3, 4\}$, $x = \{2, 3\}$)

So $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

# P-Set 1 Question 17

## Q17

Simplify

$$[A \cap (A \cap B^c)] \cup [(A \cap B) \cup (B \cap A^c)]$$

$$\begin{aligned}
&= [(A \cap A) \cap B^c] \cup [(A \cap B) \cup (B \cap A^c)] && \text{(Associative Law)} \\
&= [A \cap B^c] \cup [(A \cap B) \cup (B \cap A^c)] && \text{(Idempotent Law)} \\
&= [A \cap B^c] \cup [(B \cap A) \cup (B \cap A^c)] && \text{(Commutative Law)} \\
&= [A \cap B^c] \cup [B \cap (A \cup A^c)] && \text{(Distributive Law)} \\
&= [A \cap B^c] \cup [B \cap \mathcal{U}] && \text{(Negation Law)} \\
&= [A \cap B^c] \cup B && \text{(Identity Law)} \\
&= B \cup [A \cap B^c] && \text{(Commutative Law)} \\
&= (B \cup A) \cap (B \cup B^c) && \text{(Distributive Law)} \\
&= (B \cup A) \cap \mathcal{U} && \text{(Union with cmpt)} \\
&= B \cup A && \text{(Identity Law)}
\end{aligned}$$

# P-Set 1 Question 17

## Q17, continued

Simplify

$$[A \cap (A \cap B^c)] \cup [(A \cap B) \cup (B \cap A^c)]$$

and hence simplify

$$[A \cup (A \cup B^c)] \cap [(A \cup B) \cap (B \cup A^c)]$$

**Proof.** Observe that $[A \cup (A \cup B^c)] \cap [(A \cup B) \cap (B \cup A^c)]$ is just the **dual** of

$$[A \cap (A \cap B^c)] \cup [(A \cap B) \cup (B \cap A^c)].$$

This means that the simplified expressions of both laws are also duals of each other. Since

$$[A \cap (A \cap B^c)] \cup [(A \cap B) \cup (B \cap A^c)] = B \cup A,$$

this directly implies that

$$[A \cup (A \cup B^c)] \cap [(A \cup B) \cap (B \cup A^c)] = B \cap A.$$

# P-Set 1 Question 19

## Q19

Use the laws of set algebra to prove for any $R, P, Q$

$$(R - P) - Q = R - (P \cup Q)$$

Using the laws of set algebra,

$$\begin{aligned}
(R - P) - Q &= (R \cap P^c) \cap Q^c && \text{(Difference Law)} \\
&= R \cap (P^c \cap Q^c) && \text{(Associative Law)} \\
&= R \cap (P \cup Q)^c && \text{(De Morgan's Law)} \\
&= R - (P \cup Q) && \text{(Difference Law)}
\end{aligned}$$

# P-Set 1 Question 20(c)

## Q20(c)

Define the *symmetric difference* $A \oplus B$ of two sets $A$ and $B$ to be

$$A \oplus B = (A - B) \cup (B - A)$$

(c) Explain why $A \oplus B$ can be written as $(A \cup B) - (A \cap B)$

$$\begin{aligned}
A \oplus B &= (A - B) \cup (B - A) \\
&= (A \cap B^c) \cup (B \cap A^c) && \text{(Difference Law)} \\
&= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c] && \text{(Distributive Law)} \\
&= [B \cup (A \cap B^c)] \cap [A^c \cup (A \cap B^c)] && \text{(Commutative Law)} \\
&= [(B \cup A) \cap (B \cup B^c)] \cap [(A^c \cup A) \cap (A^c \cup B^c)] && \text{(DsLw)} \\
&= [(B \cup A) \cap \mathcal{U}] \cap [\mathcal{U} \cap (A^c \cup B^c)] && \text{(Negation Law)} \\
&= (B \cup A) \cap (A^c \cup B^c) && \text{(Identity Law)} \\
&= (A \cup B) \cap (A \cap B)^c && \text{(De Morgan's Law)} \\
&= (A \cup B) - (A \cap B) && \text{(Difference Law)}
\end{aligned}$$

# P-Set 1 Question 21

## Q21

Prove that for all sets $A$, $B$ and $C$:

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

**Proof.** Let $x = (p, q) \in A \times (B \cup C)$. This means $p \in A$ and $q \in B \cup C$. This means that $q \in B$ or $q \in C$. This means that either $p \in A$ and $q \in B$ or $p \in A$ and $q \in C$.
That is, $(p, q) = x \in A \times B$ or $(p, q) = x \in A \times C$. So, $x \in (A \times B) \cup (A \times C)$. Hence, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.
Similarly, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. (Prove in exam)

Since both sides are subsets of each other, this means that $A \times (B \cup C) = (A \times B) \cup (A \times C)$

# P-Set 1 Question 22

## Q22

Let $A_k = \{n \in \mathbb{N} \mid k \leq n \leq k^2 + 5\}$ for $k = 1, 2, 3, \ldots$. Find

(a) $\bigcup_{n=1}^{4} A_k$

(b) $\bigcap_{n=10}^{90} A_k$

a) $\bigcup_{n=1}^{4} A_k = \{1, \ldots, 6\} \cup \{2, \ldots, 9\} \cup \{3, \ldots, 14\} \cup \{4, \ldots, 21\}$

$= \{1, 2, \ldots, 20, 21\}$

b) $\bigcap_{n=10}^{90} A_k = \{10, \ldots, 105\} \cap \cdots \cap \{90, \ldots, 105, \ldots, 8105\}.$

$= \{90, 91, \ldots, 104, 105\}$

# P-Set 1 Question 26

## Q26

Prove that if $n$ is an integer, then

$$n - \left\lfloor \frac{1}{3}n \right\rfloor - \left\lfloor \frac{2}{3}n \right\rfloor$$

equals either one or zero.

Let $n = 3k$ for some $k \in \mathbb{Z}$.

$$n - \left\lfloor \frac{1}{3}n \right\rfloor - \left\lfloor \frac{2}{3}n \right\rfloor = 3k - \lfloor k \rfloor - \lfloor 2k \rfloor = 0$$

Let $n = 3k \pm 1$ for some $k \in \mathbb{Z}$,

$$3k \pm 1 - \left\lfloor k \pm \frac{1}{3} \right\rfloor - \left\lfloor 2k \pm \frac{2}{3} \right\rfloor = \begin{cases} 3k + 1 - k - 2k = 1 \\ 3k - 1 - (k - 1) - (2k - 1) = 1 \end{cases}$$

# P-Set 1 Question 28

## Q28

Let $S = \{x \in \mathbb{N} \mid 0 \leq x \leq 11\}$ and define $f : S \to S$, where $f(x) = 5n + 2 \bmod 12$. Is $f$ one-to-one? Is it onto?

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| y | 2 | 7 | 0 | 5 | 10 | 3 | 8 | 1 | 6 | 11 | 4 | 9 |

From the image above, we are able to see that not only is every $y$ unique for all $x \in S$, every single $y \in S$ is also $\in f$. Which means that $f$ is bijective.

# Cool Function Proof

**Exercise.** Prove if $f : X \to Y$ and $g : Y \to Z$ are invertible, then so is $g \circ f : X \to Z$, and the inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$.

**Proof.** For a function to be invertible, it must be bijective: one-to-one and onto. This, $f : X \to Y$ and $g : Y \to Z$ are one-to-one and onto. Now, considering $g \circ f$,

$$\begin{aligned} & (g \circ f)(x_1) = (g \circ f)(x_2) \\ \implies & f(x_1) = f(x_2) && (g \text{ is one-to-one}) \\ \implies & x_1 = x_2 && (f \text{ is one-to-one}) \end{aligned}$$

Hence, $g \circ f$ is one-to-one

Since $f$ and $g$ are onto, for every $z \in Z$, there is some $y \in Y$ such that $g(y) = z$, and for every $y \in Y$ there is one $x \in X$ such that $f(x) = y$. Hence, for every $z \in Z$, there is some $x \in X$ such that there is some $f(x) \in Y$ such that $g \circ f(x)z$. Hence $g \circ f$ is onto.

# Cool Function Proof Continued

**Proof, continued.** Since $g \circ f$ is both one-to-one and onto, it must be bijective. Hence $g \circ f$ is invertible.

Now, let the inverse of $g \circ f$ be $h : Z \to X$. Then it is evident that,

$$
\begin{aligned}
(g \circ f) \circ h &= \iota_Z && \text{(inverse functions)} \\
(g^{-1} \circ g) \circ (f \circ h) &= g^{-1} \circ \iota_Z && \text{(taking } g^{-1}\text{)} \\
\iota_Y \circ (f \circ h) &= g^{-1} \circ \iota_Z && \text{(inverse functions)} \\
f \circ h &= g^{-1} && \text{(identity function)} \\
(f^{-1} \circ f) \circ h &= f^{-1} \circ g^{-1} && \text{(taking } f^{-1}\text{)} \\
\iota_X \circ h &= f^{-1} \circ g^{-1} && \text{(inverse functions)} \\
h &= f^{-1} \circ g^{-1}. && \text{(identity function)}
\end{aligned}
$$

Hence, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

# P-Set 1 Question 44

## Q44

Using the fact that

$$\left(1-\frac{1}{k^2}\right)=\frac{(k-1)(k+1)}{k^2}$$

find an expression for $\prod_{k=2}^{N}\left(1-\frac{1}{k^2}\right)$ in terms of $N$

**Proof.** Writing out the product,

$$\prod_{k=1}^{N}\left(1-\frac{1}{k^2}\right)=\left(\frac{(1)(3)}{2^2}\right)\left(\frac{(2)(4)}{3^2}\right)\left(\frac{(3)(5)}{4^2}\right)\cdots\left(\frac{(N-1)(N+1)}{N^2}\right)$$

We observe that every term gets canceled out, except for the terms in the first and last terms in the sequence, of which only partially cancel out. Thus, the resultant expression is $(N+1)/2N$

# P-Set 2 Question 11

## Q11

Let $a, b \neq 0$ be integers. Let $S$ be the set of integers defined by

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

and let $d_0$ be the smallest integer in the set $S$.
Prove the following:

(a) If $s \in S$, then $d_0$ is a divisor of $s$

(b) $d_0$ is a divisor of both $a$ and $b$.

(c) If $d$ is a divisor of both $a$ and $b$, then $d$ is a divisor of $d_0$

(d) $d_0 = \gcd(a, b)$, and hence there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$

# 11(a)

(a) If $s \in S$, then $d_0$ is a divisor of $s$.
**Proof.** We can express $s$ in the form

$$s = d_0 q + r \qquad (r < d_0)$$

Let $d_0 = ax_0 + by_0$ and $s = ax_1 + by_1$ for some $x_0, y_0, x_1, y_1 \in \mathbb{Z}$. Then

$$\begin{aligned} s &= d_0 q + r \\ ax_1 + by_1 &= (ax_0 + by_0)q + r \\ a(x_1 - qx_0) + b(y_1 - qy_0) &= r \\ ax_2 + by_2 &= r \qquad (x_2, y_2 \in \mathbb{R}) \end{aligned}$$

which means $r \in S$. But $r < d_0$ and $d_0$ is the smallest member of $S$. This proposed a contradiction - in that $r$ doesn't exist - $r = 0$. This means $d_0 \mid s$.

# 11(b)

(b) $d_0$ is a divisor of both $a$ and $b$

**Proof.** For any $x, y \in \mathbb{Z}$ the number $ax + by \in S$.
Let $x = 0, y = 1$, then $ax + by = a \cdot 0 + b \cdot 1 = b$. This means that $b \in S$.
Let $x = 1, y = 0$, then $ax + by = a \cdot 1 + b \cdot 0 = a$. This means that $a \in S$.
And since in part a, we proved that $d \mid s$ given $s \in S$, since $a, b \in S$, it follows that $d \mid a, b$.

# 11(c)

(c) If $d$ is a divisor of both $a$ and $b$, then $d$ is a divisor of $d_0$.

**Proof.** Let $a = dm$ and $b = dn$. As established before,

$$d_0 = ax_0 + by_0.$$

So, we observe that

$$\begin{aligned} d_0 &= ax_0 + by_0 \\ &= (dm)x_0 + (dn)y_0 \\ &= d(mx_0) + d(ny_0) \\ &= d(mx_0 + ny_0) \end{aligned}$$

Thus if $d \mid a, b$ then $d$ must also be a divisor of $d_0$.

# 11(d)

(d) $d_0 = \gcd(a, b)$, and hence there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$

**Proof.** We proved that $d_0 \mid a, b$ in parts a and b. Also, considering that any $d$ that is a common factor of $a$ and $b$ satifies $d \mid d_0$, this means that $d_0$ is the largest number that is a common factor of both $a$ and $b$ or, $\gcd(a, b) = d_0$.

Since $d_0 \in S$, which is defined as

$$S = \{ax + by \mid a, b \neq 0, a, b, m, n \in \mathbb{Z}\}$$

this means that there is some $x, y \in \mathbb{Z}$ such that

$$ax + by = d_0 = \gcd(a, b)$$

# Using the Bézout's Property

## Q12

a) Prove that if $a, b, m \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a \mid m$ and $b \mid m$, then $ab \mid m$.

b) Prove that if $a$ and $b$ are coprime integers and $a \mid bc$ then $a \mid c$

a) **Proof.** By the Bézout Property, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Multiplying this by m yields

$$amx + bmy = m.$$

Since $a \mid m$ and $b \mid m$, we can say $m = aq$ and $m = bp$ for $p, q \in \mathbb{Z}$. Substituting this yields:

$$a(bp)x + b(aq)y = m.$$

$$ab(px + qy) = m$$

and since $px + qy \in \mathbb{Z}$. this means $ab \mid m$.

# Using the Bézout's Property

## Q12

a) Prove that if $a, b, m \in \mathbb{Z}$ such that $\gcd(a, b) = 1$ and $a \mid m$ and $b \mid m$, then $ab \mid m$.

b) Prove that if $a$ and $b$ are coprime integers and $a \mid bc$ then $a \mid c$

b) **Proof.** Since $a$ and $b$ are coprime, we can say $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Multiplying this by $c$ yields

$$acx + bcy = c$$

Also, since $a \mid bc$, it is true that $an = bc, n \in \mathbb{Z}$. Substituting...

$$acx + any = c$$
$$a(cx + ny) = c$$

. Since $cx + ny \in \mathbb{Z}$, this implies $a \mid c$

# Using the Bézout Property

## 7g

Prove the following for $a, b, c, d \in \mathbb{Z}$, $k, m \in \mathbb{Z}^+$:

a-f) Not important

g) If $a \equiv b \pmod{m}$ then $\gcd(a, m) = \gcd(b, m)$.

**Proof.** Since $a \equiv b \pmod{m}$, the Division Theorem states that

$$a = b + md \qquad (d \in \mathbb{Z})$$

Now, considering the expression $bx + my$, we substitute to find

$$\begin{aligned} bx_1 + my_1 &= (a - md)x + my \\ &= ax - mdx + my \\ &= ax + m(y - dx), \end{aligned}$$

which is an expression of the form $ax + my$. Since the two expressions for the Bézout Property for $a, m$ and $b, m$ are equivalent, this implies that $\gcd(a, m) = \gcd(b, m)$.