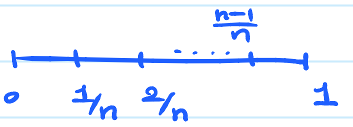
1 (I) Suppose $a_0, a_1, \ldots, a_n \in [0,1]$. Prove that for some $0 \leq i \neq j \leq n$, $\quad |a_i - a_j| \leq \frac{1}{n}$.

(Hint. Use pigeonhole principle, and 

.)

(II) Let $\alpha \in \mathbb{R}$. Prove that,

$$\forall n \in \mathbb{Z}^+, \ \exists m \in \mathbb{Z}, \ \exists k \in \mathbb{Z},$$

$$0 < m \leq n \ \wedge \ |m\alpha - k| \leq \frac{1}{n}.$$

(Hint. Let $a_i = i\alpha - \lfloor i\alpha \rfloor$ and use part (I).)

(III) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Prove that <u>for infinitely many</u> pairs of integers (m,k) we have

$$\left|\alpha - \frac{k}{m}\right| \leq \frac{1}{m^2}.$$

(Hint.

Suppose there are only finitely many such pairs:

$(m_1, k_1), \ldots, (m_s, k_s)$. Since $\alpha \notin \mathbb{Q}$, $\min\{|m_i\alpha - k_i| \mid 1 \leq i \leq s\} \neq 0$.

So for some $n \in \mathbb{Z}^+$, $\frac{1}{n} < \min\{|m_i\alpha - k_i| \mid 1 \leq i \leq s\}$.

Now use part (II), and notice $\frac{1}{n} \leq \frac{1}{m}$ if $0 < m \leq n$.)

<u>Solution</u> (I) Think about $a_0, a_1, \ldots, a_n$ as $n+1$ "pigeons" and the subintervals $[0, 1/n], [1/n, 2/n], \ldots, [\frac{n-1}{n}, 1]$ as n "pigeonholes". Since the number of "pigeons" is more than the number of pigeonholes, at least two of them should share a "pigeonhole". So $\exists\, i \neq j$ and k such that $a_i, a_j \in [\frac{k}{n}, \frac{k+1}{n}]$

$$\Longrightarrow \exists\, i \neq j, \ |a_i - a_j| \leq \frac{1}{n}.$$

(II) Let $a_i = i\alpha - \lfloor i\alpha \rfloor$ for $0 \le i \le n$. We know that for any $x \in \mathbb{R}$, $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$. So $0 \le x - \lfloor x \rfloor < 1$. Hence $a_0, a_1, \dots, a_n \in [0,1]$. Therefore by part (I) we have $\exists\, 0 \le i < j \le n$ such that $|a_i - a_j| \le 1/n$.

$$\Rightarrow \left| \left(j\alpha - \lfloor j\alpha \rfloor\right) - \left(i\alpha - \lfloor i\alpha \rfloor\right) \right| \le 1/n$$

$$\Rightarrow \Big| \underbrace{(j-i)}_{m}\alpha - \underbrace{(\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor)}_{k} \Big| \le 1/n$$

So $k = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor \in \mathbb{Z}$, and

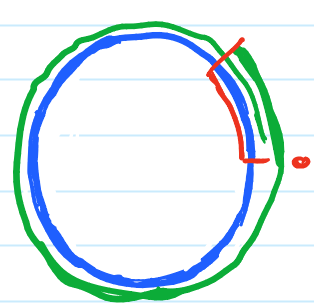
$$\left.\begin{array}{l} i<j \Rightarrow m = j-i > 0 \\ \left.\begin{array}{l} 0 \le i \\ j \le n \end{array}\right\} \Rightarrow m = j-i \le n-0 = n \end{array}\right\} \Rightarrow 0 < m \le n.$$

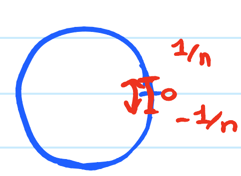
Hence we found a pair (m,k) of integers such that

① $0 < m \le n$ ② $|m\alpha - k| \le \frac{1}{n}$.

[One way to think about part (II) is using a circle with circumference 1. Now for any $x \in \mathbb{R}$ we go around this circle for "distance" x (either counterclockwise or clockwise depending on the sign of x.)

Length of the counter-clockwise arc from the initial point to the terminal point is $x - \lfloor x \rfloor$.



Part (II) essentially says one of the end points after $\alpha, 2\alpha, \dots, n\alpha$ rotations end-up in the arc 

.]

(III) [This is due to Dirichlet.] Suppose to the contrary that there are only finitely many such pair of integers. And let's list them: $(m_1, k_1), \dots, (m_s, k_s)$. So if a pair (m,k) of integers satisfy $\left|\alpha - \frac{k}{m}\right| \le \frac{1}{m^2}$ ⊛, then $(m,k) = (m_i, k_i)$ for some i.

We will use part (II) to find a new pair of integers that satisfy ⊛, and get a contradiction.

(As in the hint) since $\alpha \notin \mathbb{Q}$,

$$e = \min\{|m_1\alpha - k_1|, |m_2\alpha - k_2|, \dots, |m_s\alpha - k_s|\} > 0.$$

Choose $n \in \mathbb{Z}^+$ large enough so that $\frac{1}{n} < e$. (It is enough to choose $n > 1/e$.)

By part (I), there is a pair (m,k) of integers such that

$$\left.\begin{array}{ll} ① & 0 < m \le n \\ ② & |m\alpha - k| \le \frac{1}{n} \end{array}\right\} \Rightarrow \left|\alpha - \frac{k}{m}\right| \le \frac{1}{mn} \le \frac{1}{m^2}.$$

Hence (m,k) satisfies ⊛. So by our assumption $(m,k) = (m_i, k_i)$ for some i.

On the other hand, $|m\alpha - k| \le \frac{1}{n} < \min\{|m_1\alpha - k_1|, \dots, |m_s\alpha - k_s|\}$ which implies $|m_i\alpha - k_i| < |m_i\alpha - k_i|$, a contradiction.

[Using the circle with circumference 1 interpretation, the rotations $m_1\alpha, m_2\alpha, \dots, m_s\alpha$ are at least $\underline{e}$-away from the initial point and we are finding $0 < m \le n$ s.t. $\underline{m\alpha}$ is at most $\frac{1}{n}$-away from the initial point where $\frac{1}{n} < e$.] ■

2.(I) Prove that $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0 & \text{if } x \in \mathbb{Z}, \\ -1 & \text{if } x \notin \mathbb{Z}. \end{cases}$

(II) Prove that $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$.

Solution. We proved in class that

$$\forall x \in \mathbb{R}, \exists! m \in \mathbb{Z}, \quad m \leq x < m+1.$$

Then we called such integer m the integer part of x.

$\forall x \in \mathbb{R}, \forall m \in \mathbb{Z}, \quad m \leq x < m+1 \iff \lfloor x \rfloor = m.$

(If x is "sandwiched" between two consecutive integers and x is not equal to the larger one, then $\lfloor x \rfloor$ is the smaller integer.)

(I). $\forall x \in \mathbb{Z}, \quad x \leq x < x+1 \Rightarrow \lfloor x \rfloor = x$

$x \in \mathbb{Z} \Rightarrow -x \in \mathbb{Z} \Rightarrow \lfloor -x \rfloor = -x$

$\Rightarrow \lfloor x \rfloor + \lfloor -x \rfloor = x - x = 0.$

. Suppose $x \notin \mathbb{Z}$, and $\lfloor x \rfloor = m$. $(*)$

So $m < x < m+1$ $(x \neq m$ as $x \notin \mathbb{Z})$

$$\Rightarrow \underbrace{-m-1}_{} < -x < \underbrace{-m}_{} \Rightarrow \lfloor -x \rfloor = -m-1. \quad (**)$$

two consecutive integers.

$(*), (**) \Rightarrow \lfloor x \rfloor + \lfloor -x \rfloor = m + (-m-1) = -1.$

(II) In fact a more general statement is true:

$$\forall n \in \mathbb{Z}^+, \forall x \in \mathbb{R}, \quad \lfloor nx \rfloor = \lfloor x \rfloor + \lfloor x + \tfrac{1}{n} \rfloor + \cdots + \lfloor x + \tfrac{n-1}{n} \rfloor.$$

Here I prove this more general statement.

By Division theorem, $\exists\, q, r \in \mathbb{Z}$ such that

$$\begin{cases} \lfloor nx \rfloor = nq + r & \text{(dividing } \lfloor nx \rfloor \text{ by } n.) \\ 0 \le r < n \end{cases}$$

So $$nq + r \le nx < nq + r + 1.$$

$$\Rightarrow \quad q + \frac{r}{n} \le x < q + \frac{r+1}{n}. \quad (*)$$

To understand the right-hand side, we need to find $\lfloor x + \frac{i}{n} \rfloor$ for $0 \le i \le n-1$. So we add $\frac{i}{n}$ to all the terms of $(*)$.

$$\Rightarrow \quad q + \frac{r+i}{n} \le x + \frac{i}{n} < q + \frac{r+i+1}{n}. \quad (**)$$

Now, we consider two cases:

$\boxed{\text{Case 1.}}$ $0 \le i < n-r$

$$\left.\begin{matrix} 0 \le i \\ 0 \le r \end{matrix}\right\} \Rightarrow 0 \le r+i \Rightarrow 0 \le \frac{r+i}{n} \quad (*{*}*)$$

$$i < n-r \Rightarrow i+1 \le n-r \Rightarrow r+i+1 \le n \Rightarrow \frac{r+i+1}{n} \le 1 \quad (****)$$

$$(**), (*{*}*), (****) \Rightarrow \quad q \le x + \frac{i}{n} < q+1.$$

$$\Rightarrow \quad \lfloor x + \frac{i}{n} \rfloor = q.$$

$\boxed{\text{Case 2.}}$ $n-r \le i \le n-1$

$$n - r \le i \Rightarrow n \le r+i \Rightarrow 1 \le \frac{r+i}{n} \quad (*{*}*)'$$

$$\left.\begin{matrix} i \le n-1 \\ r < n \end{matrix}\right\} \Rightarrow r+i+1 < 2n \Rightarrow \frac{r+i+1}{n} < 2 \quad (****)'$$

$$(**), (*{*}*)', (****)' \Rightarrow \quad q+1 \le x + \frac{i}{n} < q+2$$

$$\Rightarrow \quad \lfloor x + \frac{i}{n} \rfloor = q+1.$$

Hence $\lfloor x \rfloor + \lfloor x+\frac{1}{n} \rfloor + \cdots + \lfloor x+\frac{n-r-1}{n} \rfloor + \lfloor x+\frac{n-r}{n} \rfloor + \cdots + \lfloor x+\frac{n-1}{n} \rfloor =$

$$q + q + \cdots + q + (q+1) + \cdots + (q+1) =$$

$$nq + r = \lfloor nx \rfloor . \quad \blacksquare$$

3.(I) Prove that if $f: A_1 \to A_2$ and $g: B_1 \to B_2$ are bijections, then $h: A_1 \times B_1 \to A_2 \times B_2$, $h(a,b) = (f(a), g(b))$ is a bijection.

(II) Prove that, if $A_1, \ldots, A_n$ are enumerable sets, then $A_1 \times \cdots \times A_n$ is enumerable.

(Hint. Use induction on n, and the fact that we proved in class: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is enumerable.)

Solution. (I) Injection.

$$h((a_1,b_1)) = h((a_1',b_1')) \Rightarrow (f(a_1), g(b_1)) = ((f(a_1'), g(b_1'))$$

$$\Rightarrow \left\{ \begin{array}{l} f(a_1) = f(a_1') \Rightarrow a_1 = a_1' \text{ as } f \text{ is injective} \\ g(b_1) = g(b_1') \Rightarrow b_1 = b_1' \text{ as } g \text{ is injective} \end{array} \right\} \Rightarrow (a_1,b_1) = (a_1',b_1').$$

Surjection. We have to show

$$\forall (a_2,b_2) \in A_2 \times B_2,\ \exists (a_1,b_1) \in A_1 \times B_1,\ h((a_1,b_1)) = (a_2,b_2).$$

$$\left. \begin{array}{l} \text{Since } f \text{ is surjective, } \exists a_1 \in A_1,\ f(a_1) = a_2 \\ \text{Since } g \text{ is surjective, } \exists b_1 \in B_1,\ g(b_1) = b_2 \end{array} \right\} \Rightarrow (f(a_1), g(b_1)) = (a_2, b_2)$$

$$\Rightarrow h((a_1,b_1)) = (f(a_1), g(b_1)) = (a_2,b_2).$$

(II) We proceed by induction on n.

Base. For $n=1$, there is nothing to prove.

<u>Inductive step</u>. For any $k \in \mathbb{Z}^+$,

$$\left(\underset{\text{enumerable}}{A_1, \dots, A_k} \Rightarrow \underset{\text{enumerable}}{A_1 \times \cdots \times A_k}\right) \overset{?}{\Rightarrow} \left(\underset{\text{enumerable}}{A_1, \dots, A_k, A_{k+1}} \Rightarrow \underset{\text{enumerable}}{A_1 \times \cdots \times A_{k+1}}\right).$$

By the induction hypothesis, $A_1 \times \cdots \times A_k$ is enumerable.

$\Rightarrow$ $\exists$ a bijection $A_1 \times \cdots \times A_k \xrightarrow{f} \mathbb{Z}^+$.

A_{k+1} is enumerable $\Rightarrow$ $\exists$ a bijection $A_{k+1} \xrightarrow{g} \mathbb{Z}^+$.

By part (I), $\exists$ a bijection

$$(A_1 \times \cdots \times A_k) \times A_{k+1} \xrightarrow{h} \mathbb{Z}^+ \times \mathbb{Z}^+.$$

In class we proved $\exists$ a bijection $\mathbb{Z}^+ \times \mathbb{Z}^+ \xrightarrow{i} \mathbb{Z}^+$.

Since the composite of two bijections is a bijection,

we get $A_1 \times \cdots \times A_k \times A_{k+1} \xrightarrow{i \circ h} \mathbb{Z}^+$

is a bijection. So $A_1 \times \cdots \times A_{k+1}$ is enumerable. ■

---

4. In this exercise you are allowed to use the fact that any positive integer has a unique binary representation, i.e.

$\forall n \in \mathbb{Z}^+, \exists!\ m_1, \dots, m_k \in \mathbb{Z}^{\geq 0}, \quad 0 \leq m_1 < m_2 < \cdots < m_k$

and $\quad n = 2^{m_k} + 2^{m_{k-1}} + \cdots + 2^{m_1}$.

(I) Prove that $\{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\}$ is enumerable.

(<u>Hint</u>. Let $f : \{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\} \to \mathbb{Z}^+$,

$$f(\{m_1, \dots, m_k\}) = 2^{m_1} + \cdots + 2^{m_k}.)$$

(II) Prove that there is no surjection

$$g : \{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\} \to \mathcal{P}(\mathbb{Z}^{\geq 0}),$$

where $\mathcal{P}(\mathbb{Z}^{\geq 0})$ is the power set of $\mathbb{Z}^{\geq 0}$.

Solution. (I) Let $f: \{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}, X \neq \emptyset\} \to \mathbb{Z}^+$,

$f(\{m_1, \dots, m_k\}) = 2^{m_1} + \cdots + 2^{m_k}$.

Since $\forall n \in \mathbb{Z}^+$ has a "binary representation" (as described in the hint.), $n = 2^{m_1} + \cdots + 2^{m_k}$ for some pairwise 10
distinct $m_i \in \mathbb{Z}^{\geq 0}$. Hence $n = f(\{m_1, \dots, m_k\})$. So f is surjective.

Since such "binary representation" is unique, f is injective.

We can extend f to a bijection

$$g: \{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\} \to \mathbb{Z}^+ \cup \{0\}$$

by letting $g(\emptyset) = 0$, and $g(X) = f(X)$ if $X \neq \emptyset$.

As we discussed in class, $i: \mathbb{Z}^+ \cup \{0\} \to \mathbb{Z}^+$,

$$i(n) = n+1$$

is a bijection. Hence

$$\{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\} \xrightarrow{i \circ g} \mathbb{Z}^+$$

is a bijection as the composite of two bijections is a bijection. Therefore $\{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\}$ is enumerable.

(II) Suppose to the contrary that there is a surjection

$$\{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\} \xrightarrow{h} P(\mathbb{Z}^{\geq 0}).$$

By part (I), there are bijections

$$\mathbb{Z}^{\geq 0} \to \mathbb{Z}^+ \longrightarrow \{X \subseteq \mathbb{Z}^{\geq 0} \mid X \text{ is finite}\}$$

$$n \longmapsto n-1$$

$n \longmapsto n-1$

Since composite of surjections is surjective, we get a surjection $\mathbb{Z}^{\geq 0} \longrightarrow P(\mathbb{Z}^{\geq 0})$, which contradicts Cantor's theorem. $\blacksquare$

---

5. Determine if the following functions are injective or surjective. Justify your answers.

(I) $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f((a,b)) = 3a - 2b$.

(II) Let $A \subseteq X$, and $\ell: P(X) \to P(X)$, $\ell(B) = A \Delta B$.

(Hint. What is $\ell \circ \ell(B)$?)

(III) Let Y be a non-empty subset of X, and

$r: P(X) \to P(Y)$, $r(B) = Y \cap B$.

Solution. (I) $f((0,0)) = f((2,3)) = 0$ and $(0,0) \neq (2,3)$. So f is not injective.

$\forall c \in \mathbb{Z}$, $f((c,c)) = 3c - 2c = c$. So f is surjective.

[Remark. Let $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f((x,y)) = ax + by$

Then $\mathrm{Im}(f) = \{c \in \mathbb{Z} \mid \gcd(a,b) \mid c\}$. To see this notice that $c \in \mathrm{Im}(f) \iff \exists x, y \in \mathbb{Z},\ ax + by = c$

$\iff \gcd(a,b) \mid c$ as we proved in class.

In particular f is surjective $\iff \gcd(a,b) = 1$.]

(II) $(\ell \circ \ell)(B) = \ell(\ell(B)) = A \Delta \ell(B) = A \Delta (A \Delta B)$

(

$\Rightarrow l \circ l = I_{P(X)} \Rightarrow l$ is invertible

$\Rightarrow l$ is a bijection $\Rightarrow l$ is injective and surjective.

(III) If $Y = X$, then

$$\forall A \in P(X),\ r(A) = A \cap Y = A \cap X \underset{\boxed{A \subseteq X}}{=} A.$$

$$\Rightarrow r = I_{P(X)} \Rightarrow r \text{ is a bijection.}$$

$\Rightarrow r$ is injective and surjective.

If $Y \subsetneq X$, then

- $X \setminus Y \neq \emptyset$ and $r(X \setminus Y) = (X \setminus Y) \cap Y = \emptyset$
  $r(\emptyset) = \emptyset \cap Y = \emptyset$

$\Rightarrow r$ is not injective.

- $\forall B \in P(Y) \Rightarrow \left.\begin{array}{l} B \subseteq Y \\ Y \subseteq X \end{array}\right\} \Rightarrow B \subseteq X \Rightarrow B \in P(X),$

$$r(B) = B \cap Y \underset{\boxed{B \subseteq Y}}{=} B \Rightarrow B \in \operatorname{Im}(r).$$

So r is surjective.

---

6. Suppose $f : X \to X$ is a function and $f \circ f = f$.

Prove that, $\forall x \in X$, $x \in \operatorname{Im}(f) \Leftrightarrow f(x) = x$.

<u>Solution</u>. $(\Rightarrow)$ $x \in \operatorname{Im}(f) \Rightarrow \exists x' \in X,\ x = f(x')$

$$\begin{aligned} \Rightarrow f(x) &= f(f(x')) \\ &= (f \circ f)(x') \\ &= f(x') \\ &= x. \end{aligned}$$

$(\Leftarrow)$ $x = f(x) \in \operatorname{Im}(f)$.
