Soham Chatterjee
Email: soham.chatterjee@tifr.res.in
Course: Mathematical Foundations for Computer Sciences

Assignment - 1
Dept: STCS
Date: September 7, 2024

> **Problem 1**
>
> Let $n = 17$ and consider an $n \times n$ grid of switches. A configuration of these switches can be represented by a matrix in $\{\text{OFF}, \text{ON}\}^{n\times n}$. Such a configuration can be modified by flipping any switch and its up to four adjacent switches (e.g., the you can flip the corner $(1, 1)$ and the adjacent switches $(1, 2)$ and $(2, 1)$). Show that there are configurations for which no sequence of modifications will lead the configuration where every switch is OFF. (Open ended) What can you say about other values of n? Hint: This question can be solved with linear algebra.

Solution: Since we are doing a switch ON and OFF operation we can think we are basically working in $\mathbb{F}_2$ where flipping a switch is just adding 1 mod 2. The ON state correspond to $1 \in \mathbb{F}_2$ and the OFF state correspond to $0 \in \mathbb{F}_2$. So for any state of the $n \times n$ board where some switches are ON and rest of the switches are OFF we can encode this configuration by an $n \times n$ matrix with 1 at (i, j) position if the switch at the (i, j) position of the board is ON for all $i, j \in [n]$. Now given that when we flip a switch all its adjacent switches also gets flipped. So we can encode flipping a switch at (i, j) position be a $n \times n$ matrix $A_{i,j}$ where

$$A_{i,j}[s,t] = \begin{cases} 1 & \text{if } (s,t) \in \{(i-1,j),(i,j),(i+1,j),(i,j-1),(i+1,j)\} \\ 0 & \text{otherwise} \end{cases}$$

for all $s, t \in [n]$. So flipping a switch at (i, j) position means adding $A_{i,j}$ to the configuration of the board modulo 2. We do the addition of matrices in mod2. Since flipping a switch is same as adding 1 mod 2 i.e working in $\mathbb{F}_2$. So flipping a switch 2 times is same as not flipping a switch at all. And because of $\mathbb{F}_2$ operation nature the order of sequence of flipping switches also doesn't matter. So to reach a configuration by a sequence of flipping switches we can flip any switch at most once.

With this set up to show there exists a configuration for which no sequence of flipping switches lead to every switch with OFF state with flipping any switch at most once is equivalent to the case that there exists a configuration where we can not reach by a sequence of flipping switches from every switch is OFF state with flipping any switch at most once. This is also equivalent to saying there is a $n \times n$ matrix with all entries from $\{0, 1\}$ which can be written as sum of some of the $A_{i,j}$ matrices. This is because adding $A_{i,j}$ matrix is same as flipping the (i, j) position switch and since every switch can be flipped at most once it is just the sum of some $A_{i,j}$ matrices.

Let $\mathcal{M}_n(\mathbb{F}_2)$ denote the set of all $n \times n$ matrices with each entry from $\mathbb{F}_2$. Clearly $\mathcal{M}_n(\mathbb{F}_2)$ forms a vector space over $\mathbb{F}_2$ with just matrix addition modulo 2 and multiplying a matrix with any $\alpha \in \mathbb{F}_2$ is multiplying each element of the matrix with α. So the whole problem is to show that

$$\exists\ M \in \mathcal{M}_n(\mathbb{F}_2) \text{ such that } M \notin \langle A_{i,j} \mid i,j \in [n]\rangle \iff \langle A_{i,j} \mid i,j \in [n]\rangle \neq \mathcal{M}_n(\mathbb{F}_2)$$

Hence we have to $\{A_{i,j} \mid i, j \in [n]\}$ is not a basis.

Now we have a basis $B = \{B_{i,j} \mid i, j \in [n]\}$ for $\mathcal{M}_n(\mathbb{F}_2)$ where $B_{i,j}[s, t] = 1$ if $s = i, t = j$ and 0 otherwise. $|B| = n^2$ and B is linearly independent. Clearly B is a basis for $\mathcal{M}_n(\mathbb{F}_2)$. Therefore $\dim(\mathcal{M}_n(\mathbb{F}_2)) = n^2$. And $|\{A_{i,j} \mid i, j \in [n]\}| = n^2$. Hence to show $\{A_{i,j} \mid i, j \in [n]\}$ is not a basis is same as showing they are linearly dependent.

So the problem reduced to showing the set of moves we can do on the board is linearly dependent. To show $A_n = \{A_{i,j} \mid i, j \in [n]\}$ is linearly dependent is same as showing $\exists\ M \in \mathcal{M}_n(\mathbb{F}_2)$ such that $\exists\ \{A_{i_k,j_k} \mid k \in [m_1]\} \neq \{A_{i_k,j_k} \mid k \in [m_2]\}$ such that

$$M = \sum_{k\in[m_1]} A_{i_k,j_k} = \sum_{k\in[m_2]} A_{i_k,j_k}$$

for some $m_1, m_2 \in \mathbb{N}$ with $m_1, m_2 \leq n^2$. If this happens then we will have

$$\sum_{k\in[m_1]} A_{i_k,j_k} + \sum_{k\in[m_2]} A_{i_k,j_k} = O$$

where O is all 0 matrix. So A_n is linearly dependent.

Lemma 1. *For any $n \in \mathbb{N}$ for the form $n = 6k - 1$ where $k \in \mathbb{N}$, A_n is linearly dependent.*

Proof: Let $n = 6k - 1$ for some $k \in \mathbb{N}$. Now we divide the $n \times n$ board into small rectangular boards. Consider a $n \times 2$ and $n \times 3$ boards. So we create two partitions with these rectangular boards.

$$P_1 = \Big\{[n] \times \{1, 2\}\Big\} \cup \Big\{[n] \times \{3i, 3i + 1, 3i + 2\} \mid i \in [2k - 1]\Big\}$$

And

$$P_2 = \Big\{[n] \times \{3i - 2, 3i - 1, 3i\} \mid i \in [2k - 1]\Big\} \cup \Big\{[n] \times \{n - 1, n\}\Big\}$$

We will show disjoint set of switches to be pressed for P_1 and P_2 but for both of them we will reach same configuration which is the board with $(2i - 1)^{th}$ row with all 1's for all $i \in [3k]$. Call this configuration J where for any $s, t \in [n]$

$$J[s, t] = \begin{cases} 1 & \text{when } s = 2i - 1 \text{ for some } i \in [3k] \\ 0 & \text{otherwise} \end{cases}$$

- **For P_1:** For the $[n] \times \{1, 2\}$ we press the switches $(2i - 1, 1)$ for all $i \in [3k]$. This will lead to a row with all 1's in every $(2i - 1)^{th}$ row for $i \in [3k]$ because the state of swtich at $(2i, 1)$ positions for all $i \in [3k - 1]$ will be OFF because they are flipped two times because of flipping $(2(i - 1) - 1, 1)$ and $(2i - 1, 1)$ and the $(2i, 2)$ switch state is not changed as they are unhampered. So we conclude the rectangular board $[n] \times \{1, 2\}$ after pressing all the switches of $(2i - 1, 1)$ for all $i \in [3k]$ has the $(2i - 1)^{th}$ row with all 1's for all $i \in [3k]$.

  For every $i \in [2k - 1]$ the $[n] \times \{3i, 3i + 1, 3i + 2\}$ rectangular board we press the switches $(1 + 2j, 3i + 1)$ for all $j \in [3k]$. This will lead to $(2j - 1)^{th}$ row with all 1's for all $j \in [3k]$. Because the state of the switch $(2j, 3i + 1)$ for all $j \in [3k - 1]$ will be OFF because they are flipped twice because of flipping $(2(j - 1) - 1, 3i + 1)$ and $(2j - 1, 3i + 1)$ switches and the switches are $(2j, 3i)$, $(2j, 3i + 2)$ for all $j \in [3k - 1]$ are OFF because they are not hampered because of the switches we pressed. So we conclude that the rectangular board $[n] \times \{3i, 3i + 1, 3i + 2\}$ after pressing all the switches $(2j - 1, 3i + 1)$ for all $j \in [3k]$ has the $(2j - 1)^{th}$ row with all 1's for all $j \in [3k]$ for all $i \in [2k - 1]$.

  Flipping a switch in one of the member of P_1 doesn't hamper another member because for switches on left or right edge horizontally it just one neighbor at right or left side respectively and for switches in the $n \times 3$ board we are pressing some switches in the middle column. So they don't have effect on each other. Therefore after in the $n \times n$ board if we press the switches

  $$S_1 = \{(2j - 1, 1), (2j - 1, 3i + 1) \colon i \in [2k - 1],\ j \in [3k]\}$$

  will lead to $(2j - 1)^{th}$ row with all 1's for all $j \in [3k]$. Therefore we have

  $$\sum_{j=0}^{3k} \left[A_{2j-1,1} + \sum_{i=1}^{2k-1} A_{2j-1,3i+1} \right] = J$$

- **For P_2:** For the $[n] \times \{n - 1, n\}$ we press the switches $(2i - 1, 1)$ for all $i \in [3k]$. This will lead to a row with all 1's in every $(2i - 1)^{th}$ row for $i \in [3k]$ because the state of swtich at $(2i, n)$ positions for all $i \in [3k - 1]$ will be OFF because they are flipped two times because of flipping $(2(i - 1) - 1, n)$ and $(2i - 1, n)$ and the $(2i, n - 1)$ switch state is not changed as they are unhampered. So we conclude the rectangular board $[n] \times \{n - 1, n\}$ after pressing all the switches of $(2i - 1, n)$ for all $i \in [3k]$ has the $(2i - 1)^{th}$ row with all 1's for all $i \in [3k]$.

  For every $i \in [2k - 1]$ the $[n] \times \{3i - 2, 3i - 1, 3i\}$ rectangular board we press the switches $(1 + 2j, 3i - 1)$ for all $j \in [3k]$. This will lead to $(2j - 1)^{th}$ row with all 1's for all $j \in [3k]$. Because the state of the switch $(2j, 3i - 1)$ for all $j \in [3k - 1]$ will be OFF because they are flipped twice because of flipping $(2(j-1)-1, 3i-1)$ and $(2j-1, 3i-1)$ switches and the switches are $(2j, 3i-2)$, $(2j, 3i)$ for all $j \in [3k-1]$ are OFF because they are not hampered because of the switches we pressed. So we conclude that the rectangular board $[n] \times \{3i-2, 3i-1, 3i\}$ after pressing all the switches $(2j-1, 3i-1)$ for all $j \in [3k]$ has the $(2j-1)^{th}$ row with all 1's for all $j \in [3k]$ for all $i \in [2k-1]$.

Flipping a switch in one of the member of P_1 doesn't hamper another member because for switches on left or right edge horizontally it just one neighbor at right or left side respectively and for switches in the $n \times 3$ board we are pressing some switches in the middle column. So they don't have effect on each other. Therefore after in the $n \times n$ board if we press the switches

$$S_2 = \{(2j-1, n), (2j-1, 3i-1) \colon i \in [2k-1],\ j \in [3k]\}$$

will lead to $(2j-1)^{th}$ row with all 1's for all $j \in [3k]$. Therefore we have

$$\sum_{j=0}^{3k} \left[A_{2j-1,n} + \sum_{i=1}^{2k-1} A_{2j-1,3i-1} \right] = J$$

Notice that $S_1 \cap S_2 = \phi$. Hence we get complete disjoint two sets of sequence of flipping switches S_1 and S_2 with which we reach the same configuration J. Therefore A_n is linearly independent. ■

Therefore we got that A_n is linearly dependent for all $n = 6k-1$ for any $k \in \mathbb{N}$. Therefore A_n is not a basis of $\mathcal{M}_n(\mathbb{F}_2)$. Hence there exists a configuration where we can not reach by a sequence of flipping switches. Now since the given number $17 = 6 \times 3 - 1$ i.e. it is of the form $6k-1$ we can conclude that there is an configuration where we can not reach by a sequence of flipping switches or equivalently there is an configuration for which no sequence of modifications will lead the configuration where every switch is OFF. ■

[I understood the solution of this problem from Soumyadeep Paul]

Problem 2 The Isomorphism Theorems

Let V be a vector space over a field $\mathbb{F}$. For $v \in V$ and subsets $S, T \subseteq V$, define the sets $v + S = \{v + s \mid s \in S\}$ and $S + T = \{s + t \mid s \in S, t \in T\}$.

Definition (Quotient spaces)**.** *Let $U \leq V$. Define the quotient space V/U to be the vector space over $\mathbb{F}$ whose elements are of the form $v + U$ for some $v \in V$. Addition is defined as $(v+U)+(v'+U) = (v + v' + U)$ for all $v, v' \in V$ and scalar multiplication is defined as $a(v+U) = av+U$ for all $v \in V$ and $a \in \mathbb{F}$.*

Prove that the two operations are well-defined and that V/U is indeed a vector space. Calculate its dimension. Then, prove the following theorems. After you've done so, try reading about similar isomorphism theorems for groups, rings, etc. We will discuss them later in the course.

(a) (**First isomorphism theorem**) Let U and V be two vector spaces over the same field $\mathbb{F}$ and let $\theta : U \to V$ be a linear transformation. Then, $\ker(\theta)$ is a subspace of $U, \operatorname{Im}(\theta)$ is a subspace of V, and
$$U \big/ \ker\theta \cong \operatorname{Im}\theta$$

(b) (**Second isomorphism theorem**) Let V be a vector space over a field $\mathbb{F}$ and let $S, T \leq V$. Then, $S + T \leq V$ and we have:
$$S \big/ S \cap T \cong S + T \big/ T$$

(c) (**Third isomorphism theorem**) Let $T \leq U \leq V$ be a vector spaces over the field $\mathbb{F}$. Then, $U \,/\, T \leq V \,/\, T$ and:
$$\left(V \big/ T\right) \big/ \left(U \big/ T\right) \cong V \big/ U$$

(d) (**"Fourth" isomorphism theorem**) Let $U \leq V$ be a vector spaces over the field $\mathbb{F}$. There is a bijection between subspaces of V containing U and subspaces of $V \,/\, U$.

Solution: First we will prove that $V \,/\, U$ is a vector space. We will do this step by step:

- **$(V \,/\, U, +)$ is Abelian:**
  - For any $v, v' \in V \,/\, U$ we have $(v + U) + (v' + U) = (v + v') + U$. Now $v + v' \in V$. Hence it is closed under addition
  - Let $u, v, w \in V$. Then
$$\begin{aligned}((u+U)+(v+U))+(w+U) &= ((u+v)+U)+(w+U) = ((u+v)+w)+U = (u+(v+w))+U \\ &= (w+U)+((v+w)+U) = (u+U)+((v+U)+(w+U))\end{aligned}$$
    Hence we have the associativity property.
  - $0 \in V$. So for any $v \in V$
$$(v+U)+(0+U) = (v+0)+U = v+U \quad (0+U)+(v+U) = (0+v)+U = v+U$$
    So we have the identity property as $0 + U$ is the identity element.
  - For any $v \in V$ there is $-v \in V$ since V is a vector space. Then
$$(v+U)+((-v)+U) = (v+(-v))+U = 0+U = ((-v)+v)+U = ((-v)+U)+(v+U)$$
    Hence $V \,/\, U$ also have additive identity.
  - For any $v, w \in V$ we have
$$(v+U)+(w+U) = (v+w)+U = (w+v)+U = (w+U)+(v+U)$$
    Therefore addition in $V \,/\, U$ is commutative

Hence we conclude that $(V\,/\,U, +)$ is an abelian group.

- **Multiplication:** For any $\alpha \in \mathbb{F}$, $v \in V$ we have $\alpha(v+U) = \alpha v + U$. So if $\alpha = 1$ then

$$1 \cdot (v+U) = (1 \cdot v) + U = v + U$$

and for any $\alpha, \beta \in \mathbb{F}$ we have

$$\alpha(\beta(v+U)) = \alpha((\beta v) + U) = (\alpha(\beta v)) + U = ((\alpha \cdot \beta)v) + U = (\alpha \cdot \beta)(v+U)$$

Therefore it follows the multiplication property.

- **Distributivity:** For all $v, w \in V$ and $\alpha \in \mathbb{F}$ we have

$$\begin{aligned}\alpha((v+U)+(w+U)) = \alpha((v+w)+U) = (\alpha(v+w)) + U &= (\alpha \cdot v + \alpha \cdot w) + U \\ &= ((\alpha \cdot v) + U) + ((\alpha \cdot w) + U) = \alpha(v+U) + \alpha(w+U)\end{aligned}$$

And for any $\alpha, \beta \in \mathbb{F}$ and $v \in V$ we have

$$(\alpha+\beta)(v+U) = ((\alpha+\beta)v)+U = (\alpha \cdot v + \beta \cdot v) + U = ((\alpha \cdot v)+U) + ((\beta \cdot v)+U) = \alpha(v+U) + \beta(v+U)$$

Therefore $(V\,/\,U, +, \cdot)$ follows all the properties of a vector space. Hence $V\,/\,U$ is indeed a vector space over $\mathbb{F}$.

Now we will prove all the isomorphism theorems.

(a) Define the map $\varphi : U\,/\,\ker\theta \to \operatorname{Im}\theta$ where $\varphi(x + \ker\theta) = \theta(x)$ for any $x + \ker\theta \in U\,/\,\ker\theta$ where $x \in U$. Now we will prove first φ is a well defined map then it is a linear map and then it is a bijection.

- **Well Defined:** Let $x+\ker\theta, y+\ker\theta \in U\,/\,\ker\theta$ for $x, y \in U$. Now suppose we have $x+\ker\theta = y+\ker\theta$. We have to show that $\varphi(x+\ker\theta) = \varphi(y+\ker\theta)$. Now

$$x+\ker\theta = y+\ker\theta \implies x-y \in \ker\theta \implies \theta(x-y) = 0 \implies \theta(x) = \theta(y)$$

Now we know $\theta(x) = \varphi(x+\ker\theta)$ and $\theta(y) = \varphi(y+\ker\theta)$. Hence we have $\varphi(x+\ker\theta) = \varphi(y+\ker\theta)$. So φ is a well defined map.

- **Linear Map:** Let $x+\ker\theta, y+\ker\theta \in U\,/\,\ker\theta$ for some $x, y \in U$. Then

$$\varphi((x+y)+\ker\theta) = \theta(x+y) = \theta(x) + \theta(y) = \varphi(x+\ker\theta) + \varphi(y+\ker\theta)$$

Hence φ is linear. Now let $\alpha \in \mathbb{F}$. Now

$$\varphi((\alpha x)+\ker\theta) = \theta(\alpha x) = \alpha\theta(x) = \alpha\varphi(x+\ker\theta)$$

Hence φ also satisfies the scalar multiplication property of linear maps. Hence φ is a linear map between $U\,/\,\ker\theta$ and $\operatorname{Im}\theta$.

- **Injectivity:** Let $x+\ker\theta, y+\ker\theta \in U\,/\,\ker\theta$ for some $x, y \in U$. Now suppose we have

$$\varphi(x+\ker\theta) = \varphi(y+\ker\theta) \implies \theta(x) = \theta(y) \implies \theta(x-y) = 0 \implies x-y \in \ker\theta$$

Since $x-y \in \ker\theta$ we have $y \in x+\ker\theta$ since $x-(x-y) = y$ and similarly we have $x \in y+\ker\theta$. Hence we get $x+\ker\theta = y+\ker\theta$. Therefore φ is injective.

- **Surjectivity:** Let $v \in \operatorname{Im}\theta$. Hence $\exists\ x \in U$ such that $\theta(x) = v$. Then consider the vector $x+\ker\theta \in U\,/\,\ker\theta$. Certainly we have

$$\varphi(x+\ker\theta) = \theta(x) = v$$

Hence for every $v \in \operatorname{Im}\theta$ there is an preimage $x+\ker\theta \in U\,/\,\ker\theta$ where $\varphi(x+\ker\theta) = v$. Therefore φ is surjective.

Since φ is injective and surjective we can say φ is a bijection. And since φ is also a linear map we conclude φ is an isomorphism. Therefore we have

$$U \Big/ _{\ker\theta} \cong \operatorname{Im}\theta$$

(b) Consider the map $\varphi : S \to S + T \,/\, T$ where for any $s \in S$, $s \mapsto s + T$. Now we will first show φ is a well defined surjective linear map and then we will show $\ker\varphi = S \cap T$. Then by first isomorphism theorem we will have result.

- **Well Defined:** Let $x, y \in S$ and $x = y$. Then we have to show $\varphi(x) = \varphi(y)$. Now $\varphi(x) = x + T$ and $\varphi(y) = y + T$. Now any element of $x + T$ is of the form $x + t$ for some $t \in T$. Since $x = y$ we have $x + t = y + t$. Therefore $x + t \in y + T$. And similarly for any element $y + t$ of $y + T$ for some $t \in T$ we have $y + t \in x + T$. Therefore $x + T = y + T$. Hence $\varphi(x) = \varphi(y)$. So φ is well defined.
- **Linear Map:** Let $x, y \in S$. Now

$$\varphi(x + y) = (x + y) + T = (x + T) + (y + T) = \varphi(x) + \varphi(y)$$

Let $\alpha \in \mathbb{F}$. Hence Then we have

$$\varphi(\alpha x) = (\alpha x) + T = \alpha(x + T) = \alpha\varphi(x)$$

Therefore φ is a linear map.
- **Surjectivity:** Any vector of $S + T \,/\, T$ is of the form $u + T$ for some $u \in S + T$. Now any vector of $S + T$ is of the form $s + t$ for some $s \in S$ and $t \in T$. Therefore

$$u + T = (s + t) + T = s + (t + T) = s + T$$

Now $\varphi(s) = s + T = u + T$. Therefore φ is a surjective linear map.
- **$\ker\varphi = S \cap T$:** Let $s \in S$ and $\varphi(s) = 0$. Now $\varphi(s) = s + T$. Hence $s + T = 0 + T \implies s \in T$. Therefore $s \in S \cap T$. Therefore $\ker\varphi \subseteq S \cap T$. Now let $s \in S \cap T \implies s \in T$. So $s + T = 0 + T$. Therefore $\varphi(s) = 0$. Hence $s \in \ker\varphi$. Therefore $\ker\varphi \supseteq S \cap T$. Hence we get $\ker\varphi = S \cap T$.

Therefore using the first isomorphism theorem we have

$$S \Big/ _{\ker\varphi} \cong \operatorname{Im}\varphi \iff S \Big/ _{S \cap T} \cong S + T \Big/ _{T}$$

(c) Consider the map $\varphi : V \,/\, T \to V \,/\, U$ where $v + T \mapsto v + U$ for some $v + T \in V \,/\, T$ where $v \in V$. Now we will show φ is a well defined, linear, surjective map and its kernel is $U \,/\, T$. Then we will use the first isomorphism theorem

- **Well Defined:** Let $v + T, w + T \in V \,/\, T$ for some $v, w \in V$. Now assume $v + T = w + T$. We will show $\varphi(v + T) = \varphi(w + T)$. Now $v + T = w + T \implies v - w \in T$. And we have $T \leq U$. Therefore

$$v - w \in U \implies v + U = w + U \implies \varphi(v) = \varphi(w)$$

Therefore φ is well defined.
- **Linear Map:** Let $v + T, w + T \in V \,/\, T$ for some $v, w \in V$. Now

$$\varphi((v + w) + T) = (v + w) + U = (v + U) + (w + U) = \varphi(v + T) + \varphi(w + T)$$

Let $\alpha \in \mathbb{F}$. Then we have

$$\varphi((\alpha v) + T) = (\alpha v) + U = \alpha(v + U) = \alpha\varphi(v)$$

Therefore φ is a well defined linear map.

- **Surjectivity:** Let $v + U \in V \,/\, U$ for some $v \in V$. Since $T \leq U$, $v + T$ is a vector of $V \,/\, T$. Then $\varphi(v + T) = v + U$. Therefore φ is surjective.
- **$\ker \varphi = U \,/\, T$:** Let $v + T \in \ker \varphi$ for some $v \in V$. Now $\varphi(v + T) = 0$. Hence $v + U = 0 + U \implies v \in U$. Therefore $v + T \in U \,/\, T$ as $U \,/\, T \leq V \,/\, T$. Hence $\ker \varphi \subseteq U \,/\, T$. Now let $u + T \in U \,/\, T$ for some $u \in U$. Since $U \,/\, T \leq V \,/\, T$, $u + T \in V \,/\, T$. Now $\varphi(u + T) = u + U = o + U$. Therefore $u + T \in \ker \varphi$. Therefore we have $\ker \varphi \supseteq U \,/\, T$. Hence we have
$$\ker \varphi = {}^{U}\!\big/_{T}$$

Therefore using first isomorphism theorem we have

$$\left({}^{V}\!\big/_{T}\right)\Big/_{\ker \varphi} \cong \operatorname{Im} \varphi \iff \left({}^{V}\!\big/_{T}\right)\Big/\left({}^{U}\!\big/_{T}\right) \cong {}^{V}\!\big/_{U}$$

(d) Consider the set $\operatorname{Spec}(V)_U = \{W \leq V \mid W \text{ subspace of } V \text{ containing } U\}$ for any vector space V over $\mathbb{F}$. Also consider the set $\operatorname{Spec}(V \,/\, U) = \{W \leq V \,/\, U \mid W \text{ subspace of } V \,/\, U\}$. Now we have to show there is a bijection between $\operatorname{Spec}(V)_U$ and $\operatorname{Spec}(V \,/\, U)$. Consider the function $f : \operatorname{Spec}(V)_U \to \operatorname{Spec}(V \,/\, U)$ where $W \mapsto W \,/\, U$ for any subspace $W \in \operatorname{Spec} V_U$. Now we will show f is a bijection.

- **Injectivity:** Now let $S, T \in \operatorname{Spec}(V)_U$ such that $f(S) = f(T)$. Hence we have $S \,/\, U = T \,/\, U$. Let $s \in S$. Then $s + U \in S \,/\, U$. Therefore $s + U \in T \,/\, U$. So $s + U = t + U$ for some $t \in T$. Now we have $s \in t + U \subseteq t + T = T$. So $s \in T$. Therefore $S \subseteq T$. Similarly for any $t \in T$ we have
$$t + U \in {}^{T}\!\big/_{U} = {}^{S}\!\big/_{U} \implies t + U = s + U \text{ for some } s \in S \implies t \in s + U \subseteq s + S = S \implies T \subseteq S$$
Therefore we have $S = T$. Hence f is injective.
- **Surjectivity:** Let $W \leq V \,/\, U$. Consider the linear map $\psi : V \to V \,/\, U$ where $v \mapsto v + U$ for all $v \in V$. Now ψ is indeed a linear map because of the addition and scaler multiplication rules in $V \,/\, U$ explained in defining quotient space as
$$\psi(v + w) = (v + w) + U = (v + U) + (w + U) = \psi(v) + \psi(w) \text{ for all } v, w \in V$$
and
$$\psi(\alpha v) = (\alpha v) + U = \alpha(v + U) = \alpha\psi(v) \text{ for all } \alpha \in \mathbb{F} \text{ and } v \in V$$
Then consider the subspace $\psi^{-1}(W)$ of V. Then we
$$\varphi\left(\psi^{-1}(S)\right) = \varphi\left(\{v \in V \mid v + U \in W\}\right) = \{\varphi(v) \mid v \in V,\ v + U \in W\} = W$$

Therefore f is bijective. Hence there is a bijection between subspaces of V containing U and subspaces of $V \,/\, U$.

■

Problem 3

Let V be a vector space over a field $\mathbb{F}$ and $W_1, \dots, W_k \leq V$ be subspaces. We say that V is the internal direct sum of $W_1, \dots, W_k$ and write $V = \bigoplus_{i=1}^{k} W_i$ if for all $v \in V$, there exists unique $w_1 \in W_1, \dots, w_k \in W_k$ such that $v = \sum_{i=1}^{k} w_i$. The values $w_1, \dots, w_k$ are called the projections of v onto $W_1, \dots, W_k$ respectively.

- Show that $V = \bigoplus_{i=1}^{k} W_i$ if and only if $V = \sum_{i=1}^{k} W_i$, and for all $i \in [k]$, we have $W_i \cap \sum_{i' \neq i} W_{i'} = \{0\}$.
- Let $\theta \in L(V)$. Show that θ is idempotent (namely, we have $\theta \circ \theta = \theta$) if and only if $V = \operatorname{Im}(\theta) \oplus \ker(\theta)$ and for all $v \in V, \theta(v)$ is just the projection of v onto $\operatorname{Im}(\theta)$.
- Let $\theta_1, \dots, \theta_k \in L(v)$ be idempotent such that $\theta_i \circ \theta_{i'} = 0$ whenever $i \neq i' \in [k]$. Let $\theta_0 = I - \sum_{i=1}^{k} \theta_i$. Show that θ_0 is idempotent and:

$$V = \bigoplus_{i=0}^{k} \operatorname{Im}(\theta_i)$$

Solution:

- – **Forward Direction ($\Rightarrow$):** $V = \bigoplus_{i=1}^{k} W_i$. Then for all $v \in V$, $\exists!\ w_i \in W_i$ such that $v = \sum_{i=1}^{n} w_i$. So $v \in \sum_{i=1}^{k} W_i \implies V \subseteq \sum_{i=1}^{k} W_i$. Now since W_i is a subspace of V for all $i \in [k]$, $\sum_{i=1}^{k} W_i$ is a subspace of V. Therefore we have $V = \sum_{i=1}^{k} W_i$.

  Now suppose $\exists\ i \in [k]$ such that $W_i \cap \sum_{i' \neq i} W_{i'} \neq \{0\}$. Let $w \in W_i \cap \sum_{i' \neq i} W_{i'}$ and $w \neq 0$. Since $w \in \sum_{i' \neq i} W_{i'}$ there exists $w_{i'} \in W_{i'}$ for all $i' \in [k]$, $i' \neq i$ such that $w = \sum_{i' \neq i} w_{i'}$. Hence we have two ways of expressing $w \in V$ one is as a vector of W_i and another is $\sum_{i' \neq i} w_{i'}$. This contradicts that for all $v \in V$ there exists unique $w_i \in W_i$ for all $i \in [k]$ such that $v = \sum_{i=1}^{k} w_i$. Hence contradiction. We have for all $i \in [k]$, $W_i \cap \sum_{i' \neq i} W_{i'} = \{0\}$.

  – **Backward Direction ($\Leftarrow$):** Let $V = \sum_{i=1}^{k} W_i$ and for all $i \in [k]$, $W_i \cap \sum_{i' \neq i} W_{i'} = \{0\}$. For all $v \in V = \sum_{i=1}^{k} W_i$ there exists $w_i \in W_i$ for all $i \in [k]$ such that $v = \sum_{i=1}^{k} w_i$. Suppose there exists a vector $v \in V$ such that $\exists\ \{w_i \in W_i \mid i \in [k]\} \neq \{w'_i \in W_i \mid i \in [k]\}$ such that

$$v = \sum_{i=1}^{k} w_i = \sum_{i=1}^{k} w'_i \implies \sum_{i=1}^{k} (w_i - w'_i) = 0 \implies w_i - w'_i = \sum_{j \neq i} (w'_j - w_j)$$

  So denote $w = w_i - w'_i$ Then $w \in W_i$ and $w \in \sum_{j \neq i} W_j$ as $w'_j - w_j \in W_j$ for all $j \in [k]$, $j \neq i$ and $\sum_{j \neq i} (w'_j - w_j) \in \sum_{j \neq i} W_j$. So $W_i \cap \sum_{j \neq i} W_j \neq \{0\}$. Hence contradiction. There doesn't exists any vector in V with more than one representations as summation of k vectors one from each of the W_i, $i \in [k]$. Hence for each $v \in V$, $\exists!\ w_i \in W_i\ \forall\ i \in [k]$ such that $v = \sum_{i=1}^{k} w_i$. Hence $V = \bigoplus_{i=1}^{k} W_i$.

Hence we have $V = \bigoplus_{i=1}^{k} W_i \iff V = \sum_{i=1}^{k} W_i$, and for all $i \in [k]$, we have $W_i \cap \sum_{i' \neq i} W_{i'} = \{0\}$.

- - **Forward Direction ($\Rightarrow$):** Let $\theta \in L(V)$ is idempotent. Suppose $v \in V$ be any vector. Now we have $v = \theta(v) + (v - \theta(v))$. Certainly $\theta(v) \in \operatorname{Im}\theta$. Now

$$\theta(v - \theta(v)) = \theta(v) - T \circ \theta(v) = \theta(v) - \theta(v) = 0 \implies v - \theta(v) \in \ker\theta$$

  Hence for all $v \in V$, v can be expressed as a sum of a vector from $\operatorname{Im}\theta$ and a vector from $\ker\theta$. Hence $V \subseteq \operatorname{Im}\theta + \ker\theta$ and since $\operatorname{Im}\theta$ and $\ker\theta$ are subspaces of V so we have $V = \operatorname{Im}\theta + \ker\theta$. Now it is enough to show that $\ker\theta \cap \operatorname{Im}\theta = \{0\}$. Now let $v \in \ker\theta \cap \operatorname{Im}\theta$. Since $v \in \ker\theta$ we have $\theta(v) = 0$. And $v \in \operatorname{Im}\theta$ so there exists $u \in V$ such that $\theta(u) = v$. Therefore $0 = \theta(v) = \theta \circ \theta(u) = \theta(u) = v$. Hence $\ker\theta \cap \operatorname{Im}\theta = \{0\}$. Therefore by the part (a) we have $V = \ker\theta \oplus \operatorname{Im}\theta$. Hence for all $v \in V$, $v = \theta(v) + (v - \theta(v))$ is the only unique representation as a sum of a vector from $\operatorname{Im}\theta$ and a vector from $\ker\theta$. Hence $\theta(v)$ is the projection of v onto $\operatorname{Im}(\theta)$.

  - **Backward Direction ($\Leftarrow$):** Suppose $V = \operatorname{Im}\theta \oplus \ker\theta$. For any $v \in V$, $\exists!\ u \in \operatorname{Im}\theta,\ w \in \ker\theta$, such that $v = u + w$. Since $\theta(v)$ is the projection of v onto $\operatorname{Im}\theta$ we have $u = \theta(v)$. Then $v = \theta(v) + w$ where $\theta(w) = 0$. Hence we have

$$\theta(v) = \theta(\theta(v) + w) = \theta \circ \theta(v) + \theta(w) = \theta \circ \theta(v)$$

  Hence we have for all $v \in V$, $\theta(v) = \theta \circ \theta(v)$. Therefore $\theta \circ \theta = \theta$ i.e. θ is idempotent.

Hence we have θ is idempotent $\iff V = \operatorname{Im}\theta \oplus \ker\theta$ and for all $v \in V$, $\theta(v)$ is just the projection of v onto $\operatorname{Im}\theta$.

- - We know for all $i \in [k]$ $\theta_i \circ \theta_i = \theta_i$ and for all $i, j \in [k]$, $i \neq j$ we have $\theta_i \circ \theta_j = 0$. Now

$$\begin{aligned}
\theta_0 \circ \theta_0 &= \left[I - \sum_{i=1}^{k} \theta_i\right] \circ \left[I - \sum_{j=1}^{k} \theta_j\right] \\
&= I \circ I - I \circ \left(\sum_{i=1}^{k} \theta_i\right) - \left(\sum_{j=1}^{k} \theta_j\right) \circ I + \left(\sum_{i=1}^{k} \theta_i\right) \circ \left(\sum_{j=1}^{k} \theta_j\right) \\
&= I - \sum_{i=1}^{k} \theta_i - \sum_{i=1}^{k} \theta_i + \left(\sum_{i=1}^{k} \theta_i\right) \circ \left(\sum_{j=1}^{k} \theta_j\right) \\
&= I - 2\sum_{i=1}^{k} \theta_i + \sum_{1 \leq i,j \leq k} \theta_i \circ \theta_j \\
&= I - 2\sum_{i=1}^{k} \theta_i + \sum_{i=1}^{k} \theta_i \circ \theta_i + \sum_{1 \leq i \neq j \leq \leq k} \theta_i \circ \theta_j \\
&= I - 2\sum_{i=1}^{k} \theta_i + \sum_{i=1}^{k} \theta_i \circ \theta_i = I - 2\sum_{i=1}^{k} \theta_i + \sum_{i=1}^{k} \theta_i = I - \sum_{i=1}^{k} \theta_i = \theta_0
\end{aligned}$$

  Hence we have θ_0 is idempotent.

  - Now we have to show $V = \bigoplus_{i=0}^{k} \operatorname{Im}\theta_i$. First of all notice for all $i \in [k]$ we have

$$\theta_i \circ \theta_0 = \theta_i \circ \left(I - \sum_{j=1}^{k} \theta_j\right) = \theta_i - \sum_{j=1}^{k} \theta_i \circ \theta_j = \theta_i - \theta_i \circ \theta_i = 0$$

And similarly

$$\theta_0 \circ \theta_i = \left(I - \sum_{j=1}^{k} \theta_j\right) \circ \theta_i = \theta_i - \sum_{j=1}^{k} \theta_j \circ \theta_i = \theta_i - \theta_i \circ \theta_i = 0$$

Therefore $\forall\ i, j \in \{0, 1, \dots, k\}$ we have $\theta_i \circ \theta_j = 0$ if $i \neq j$ and $\theta_i \circ \theta_i = \theta_i$. Now by part (b) we have $V = \ker \theta_0 \oplus \operatorname{Im} \theta_0$. We will show $\ker \theta_0 = \bigoplus_{i=1}^{k} \operatorname{Im} \theta_i$.

Lemma 2. *For all $v \in \ker \theta_0$, $v = \sum_{i=1}^{k} \theta_i(v)$*

Proof: $\theta_0(v) = \left(I - \sum_{i=1}^{k} \theta_i\right)(v) = v - \sum_{i=1}^{k} \theta_i(v)$. Since $v \in \ker \theta_0$ we have

$$v - \sum_{i=1}^{k} \theta_i(v) = 0 \iff v = \sum_{i=1}^{k} \theta_i(v)$$

■

Now $\theta_i(v) \in \operatorname{Im} \theta_i$. Therefore $\ker \theta_0 \subseteq \sum_{i=1}^{k} \operatorname{Im} \theta_i$. Also for any $v \in \sum_{i=1}^{k} \operatorname{Im} \theta_i$, v can be written as $\sum_{i=1}^{k} w_i$ where $w_i \in \operatorname{Im} \theta_i$. Therefore we can think $w_i = \theta_i(v_i)$ for some $v \in V$. Therefore $v = \sum_{i=1}^{k} \theta_i(v_i)$. Hence

$$\theta_0(v) = \sum_{i=1}^{k} \theta_0 \circ \theta_i(v_i) = 0$$

Hence $v \in \ker \theta_0$. Hence $\sum_{i=1}^{k} \operatorname{Im} \theta_i \subseteq \ker \theta_0$. Hence we get $\ker \theta_0 = \sum_{i=1}^{k} \operatorname{Im} \theta_i$. Now it is enough to show that $\forall\ i \in [k]$ we have $\operatorname{Im} \theta_i \cap \left(\sum_{j \neq i} \operatorname{Im} \theta_j\right) = \{0\}$.

Lemma 3. $\forall\ i \in [k]$ *we have* $\operatorname{Im} \theta_i \cap \left(\sum_{j \neq i} \operatorname{Im} \theta_j\right) = \{0\}$

Proof: For any $i \in [k]$, let $v \in \operatorname{Im} \theta_i \cap \left(\sum_{j \neq i} \operatorname{Im} \theta_j\right)$. Since $v \in \operatorname{Im} \theta_i$ there exists $u \in V$, such that $v = \theta_i(u)$. Now since $v \in \sum_{j \neq i} \operatorname{Im} \theta_j$, $\exists\ u_j \in V$ for all $j \in [k]$ such that $v = \sum_{j \neq i} \theta_j(u_j)$. Now

$$\theta_i(v) = \sum_{j \neq i} \theta_i\left(\theta_j(u_i)\right) = \sum_{j \neq i} \theta_i \circ \theta_j(u_j) = 0$$

So $\theta_i(v) = 0$ but $\theta_i(v) = \theta_i\left(\theta_i(u)\right) = \theta_i \circ \theta_i(u) = \theta_i(u) = v$. Therefore $v = 0$. Hence we have $\operatorname{Im} \theta_i \cap \left(\sum_{j \neq i} \operatorname{Im} \theta_j\right) = \{0\}$ ■

Hence by part (a) and Lemma 2, Lemma 3 we have $\ker \theta_0 = \bigoplus_{i=1}^{k} \operatorname{Im} \theta_i$. Hence we have $V = \bigoplus_{i=0}^{k} \operatorname{Im} \theta_i$.

■

> **Problem 4**
>
> Let V be a 3-dimensional vector space over the field $\mathbb{Q}$ of rationals. Let $\theta \in L(V)$ and $x \neq 0 \in V$ be such that $\theta(x) = y, \theta(y) = z$, and $\theta(z) = x + y$. Show that x, y, z form a basis of V.

Solution: First we will show 2 lemmas. Then using them we will show x, y, z form a basis.

Lemma 4. $\theta(z) \neq 0$

Proof: If $\theta(z) = 0$ then we have $x + y = 0 \implies y = -x$. That means $\theta(x) = y = -x$. Therefore $\theta(y) = \theta(-x) = -\theta(x) = -(-x) = x$. Therefore $z = x$. Then $\theta(z) = \theta(x) = y = -x$. We have

$$\theta(z) = 0 \implies -x = 0 \implies x = 0$$

But given that $x \neq 0$. Hence contradiction. So $\theta(z) \neq 0$. ■

By the lemma we also have $y, z \neq 0$ because otherwise we will have $\theta(z) = 0$ which is not possible. Hence $x, y = \theta(x), z = \theta(y), \theta(z)$ all of them are nonzero.

Lemma 5. *x is not an eigenvector of θ.*

Proof: Suppose x is an eigenvector of θ. Then $\exists\ \lambda \in \mathbb{Q}$ such that $\theta(x) = \lambda x$. By Lemma 4 we have $\lambda \neq 0$. Hence $\theta(x) = \lambda x = y$. $\theta(y) = \theta(\lambda x) = \lambda^2 x = z$. And we have $\theta(z) = \theta(\lambda^2 x) = \lambda^3 x$. Therefore we have

$$\lambda^3 x = x + y = x + \lambda x \iff x(\lambda^3 - \lambda - 1) = 0 \iff \lambda^3 - \lambda - 1 = 0$$

Now we will show the polynomial $f(t) = t^3 - t - 1$ does not have any rational root. Suppose $f(t)$ Let $\frac{p}{q}$ be a rational root of $f(t)$ where $\frac{p}{q}$ is in the lowest form for some $p, q \in \mathbb{Z}$ with $q \neq 0$ and p, q coprime. Then

$$f\left(\frac{p}{q}\right) = \frac{p^3}{q^3} - \frac{p}{q} - 1 = 0 \iff p^3 - pq^2 - q^3 = 0$$

Call $f' = p^3 - pq^2 - q^3$. Now $q \mid 0$, $q \mid q^3$, $q \mid pq^2$. Hence

$$q \mid f' + q^3 + pq^2 \implies q \mid p^3 \implies q = 1$$

Here $q = \pm 1$ since $gcd(p, q) = 1$. Similarly $p \mid 0$, $p \mid p^3$, $p \mid pq^2$. Hence

$$p \mid p^3 - pq^2 - f' \implies p \mid q^3 \implies p = \pm 1$$

Hence both $p, q \in \{1, -1\}$. So 1 or -1 should be a root of $f(t)$ but it is not. Hence contradiction. $f(t)$ has no rational root.

Since $f(t)$ has no rational root there doesn't exists any $\lambda \in \mathbb{Q}$, $\lambda \neq 0$ such that λ is an eigenvalue of θ. Hence contradiction. Therefore x is not an eigenvector of θ. ■

Now we are ready to prove that x, y, z forms a basis. Showing x, y, z are linearly independent is enough for us. Suppose they are not. Then $\exists\ a, b, c \in \mathbb{Q}$ not all zero such that $ax + by + cz = 0$. WLOG asssume $c \neq 0$. Hence we can divide a, b by c and still get a rational. So we can think $\exists\ a, b \in \mathbb{Q}$ such that

$$ax + by - z = 0 \iff z = ax + by$$

Now composing θ on both sides we have

$$a\theta(x) + b\theta(y) - \theta(z) = 0 \iff ay + bz - (x + y) = 0 \implies -x + (a - 1)y + bz = 0$$

Now replacing value of z here we have

$$-x + (a - 1)y + bz = 0 \iff -x + (a - 1)y + b(ax + by) = 0 \iff (ab - 1)x + (a + b^2 - 1)y = 0$$

Case 1 ($\boldsymbol{ab-1,\ a+b^2-1\neq 0}$): If both of $ab-1$ and $a+b^2-1$ is nonzero then $y=\frac{1-ab}{a+b^2-1}x \implies x$ is an eigenvector of θ. This is not possible by Lemma 5. So at least one of them is zero. Suppose exactly one of them zero.

Case 2 ($\boldsymbol{ab-1=0,\ a+b^2-1\neq 0}$): Then $(a+b^2-1)y=0 \implies y=0$ then we have $\theta(z)=0$ which contradicts Lemma 4.

Case 3 ($\boldsymbol{ab-1\neq 0,\ a+b^2-1=0}$): Then $(ab-1)x=0 \implies x=0$. But given that $x\neq 0$. Therefore this case is not possible.

Case 4 ($\boldsymbol{ab-1=a+b^2-1=0}$): In this case

$$ab-1=0 \iff b=\frac{1}{a} \implies a+b^2-1=0 \iff a+\frac{1}{a^2}-1==0 \iff a^3+1-a^2=0$$

Consider the polynomial $g(w)=w^3-w^2+1$. So a is a root of $g(w)$. Now let again $a=\frac{s}{t}$ in their lowest form. Then

$$g\left(\frac{s}{t}\right)=\frac{s^3}{t^3}-\frac{s^2}{t^2}+1=0 \iff s^3-s^2t+t^3=0$$

Call $g'=s^3-s^2t+t^3$. Then we have

$$s \mid g'-s^3+s^2t \implies s \mid t^3$$

Since $gcd(s,t)=1$ we have $s=\pm 1$. Again

$$t \mid g'-t^3+s^2t \implies t \mid s^3 \implies t=\pm 1$$

Hence we have $a=\pm 1$. But 1 or -1 both of them are not root of $g(w)$. Therefore both $ab-1$ and $a+b^2-1$ can not be both zero.

Therefore none of cases is possible. Hence contradiction. Such a,b does not exist. Therefore x,y,z are linearly independent. ■

Problem 5

Show that the set of real numbers $\mathbb{R}$ with standard operations forms a vector space over the field of rationals $\mathbb{Q}$. This is an example of an infinite-dimensional vector space, as we shall now see in two different ways.

- Show that for any $k > 0$ and any primes $p_1, \ldots, p_k$, the real numbers $\log p_1, \ldots, \log p_k$ are linearly independent over $\mathbb{Q}$.
- Show that for any $k > 0$ there is a one-to-one function mapping $\mathbb{Q}^k$ to $\mathbb{Q}$.

For both of the above, why do we get that $\mathbb{R}$ forms an infinite-dimensional vector space over $\mathbb{Q}$?

Solution: First we will prove $\mathbb{R}$ forms a vector space over $\mathbb{Q}$. We already know $(\mathbb{R}, +)$ is an abelian group. So we only need to show that it follows the multiplication and distributivity property.

- **Multiplication:** For any $\alpha \in \mathbb{Q}$, $x \in \mathbb{R}$, $\alpha \in \mathbb{Q} \implies \alpha \in \mathbb{R}$. Hence $\alpha x \in \mathbb{R}$ as multiplication of two reals is real. So if $\alpha = 1$ then

$$1 \cdot x = x$$

and for any $\alpha, \beta \in \mathbb{Q} \implies \alpha, \beta \in \mathbb{R}$ we have

$$\alpha(\beta x) = \alpha\beta x = (\alpha \cdot \beta)x$$

Therefore it follows the multiplication property.

- **Distributivity:** For all $x, y \in \mathbb{R}$ and $\alpha \in \mathbb{Q}$ we have $\alpha(x + y) = \alpha x + \alpha y$ as $\alpha \in \mathbb{Q} \implies \alpha \in \mathbb{R}$ and $\mathbb{R}$ follows the distributive property. Similarly for any $\alpha, \beta \in \mathbb{Q} \implies \alpha, \beta \in \mathbb{R}$ and $x \in \mathbb{R}$ we have $(\alpha + \beta)x = \alpha x + \beta x$. Hence $\mathbb{R}$ follows the distributive property over $\mathbb{Q}$.

Therefore $(\mathbb{R}, +, \cdot)$ follows all the properties of a vector space over $\mathbb{Q}$. . Hence $\mathbb{R}$ is indeed a vector space over $\mathbb{Q}$.

Now we will see two different ways to prove that $\mathbb{R}$ is an infinite-dimensional vector space over $\mathbb{Q}$.

- Let $a_i \in \mathbb{Q}$ for all $i \in [k]$ such that $\sum\limits_{i=1}^{k} a_i \log p_i = 0$. Now

$$\sum_{i=1}^{k} a_i \log p_i = \sum_{i=1}^{k} \log p_i^{a_i} = \log \left[\prod_{i=1}^{k} p_i^{a_i}\right]$$

Since

$$\sum_{i=1}^{k} a_i \log p_i = 0 \iff \log \left[\prod_{i=1}^{k} p_i^{a_i}\right] = 0 \iff \prod_{i=1}^{k} p_i^{a_i} = 1$$

Let for each $i \in [k]$, $a_i = \frac{m_i}{n_i}$ where $m_i, n_i \in \mathbb{Z}$, $n_i \neq 0$ and $gcd(m_i, n_i) = 1$. Let

$$b_i = a_i \prod_{j=1}^{k} n_j = \frac{m_i}{n_i} \prod_{j=1}^{k} n_j = m_i \prod_{j \neq i} n_j \in \mathbb{Z}$$

Then we have

$$1 = \prod_{i=1}^{k} p_i^{a_i} = \left(\prod_{i=1}^{k} p_i^{a_i}\right)^{\prod\limits_{j=1}^{k} n_j} = \prod_{i=1}^{k} p_i^{a_i \prod\limits_{j=1}^{k} n_j} = \prod_{i=1}^{k} p_i^{b_i} = 1$$

Hence we are getting product of some integral powers of first k primes is 1. This is not possible unless all the powers are zero because primes doesn't divide each other. So unless the powers are zero there is no way canceling prime power by a bunch of other prime powers. Hence for all $i \in [k]$, $b_i = 0 \iff a_i = 0$ since $\forall\ i \in [k]$, $n_i \neq 0$. Hence $\{\log p_i\}_{i \in [k]}$ are linearly independent. Since k is arbitrary, we have for all $k \in \mathbb{N}$ and for any primes $p_1, \ldots, p_k$ the real numbers $\log p_1, \ldots, \log p_k$ are linearly independent over $\mathbb{Q}$.

Proof of $\mathbb{R}$ is Infinite-Dimensional over $\mathbb{Q}$: Suppose $\mathbb{R}$ is not infinite-dimensional over $\mathbb{Q}$. Let dimension of $\mathbb{R}$ over $\mathbb{Q}$ is $n \in \mathbb{N}$. Then suppose $p_1, \ldots, p_{n+1}$ be any $n+1$ prime numbers. By the above we have that $\log p_1, \ldots, \log p_{n+1}$ are linearly independent over $\mathbb{Q}$. But $\dim \mathbb{R} = n$ over $\mathbb{Q}$. So $\mathbb{R}$ can not have a set of linearly independent vectors with size more than its dimension. Hence contradiction. $\mathbb{R}$ can not be a finite-dimensional vector space over $\mathbb{Q}$. Therefore $\mathbb{R}$ is an infinite-dimensional vector space over $\mathbb{Q}$.

- For any $k > 0$ consider the function $f_k : \mathbb{Q}^k \to \mathbb{Q}$ where for any $(q_1, \ldots, q_k) \in \mathbb{Q}$. Let n_i denote the i^{th} prime number. Let $q_i = \frac{a_i}{b_i}$ where $a_i \in \mathbb{Z}$, $b_i \in \mathbb{N}$, $b_i \neq 0$ and $gcd(a_i, b_i) = 1$. Then we define the map

$$f_k(q_1, \ldots, q_k) = \prod_{i=1}^{k} n_{2i-1}^{a_i} n_{2i}^{b_i}$$

We have to show that this map is injective. Supose $f(p_1, \ldots, p_k) = f(q_1, \ldots, q_k)$. Let $p_i = \frac{a_i}{b_i}$ and $q_i = \frac{c_i}{d_i}$ with $a_i, b_i, c_i, d_i \in \mathbb{Z}$ with $b_i, d_i \neq 0$ for all $i \in [k]$ and $gcd(a_i, b_i) = 1 = gcd(c_i, d_i)$. Now

$$\begin{aligned} f(p_1, \ldots, p_k) = f(q_1, \ldots, q_k) &\iff \prod_{i=1}^{k} n_{2i-1}^{a_i} n_{2i}^{b_i} = \prod_{i=1}^{k} n_{2i-1}^{c_i} n_{2i}^{d_i} \\ &\iff \prod_{i=1}^{k} n_{2i-1}^{a_i - c_i} n_{2i}^{b_i - d_i} = 1 \end{aligned}$$

Hence we are getting product of some integral powers of first k primes is 1. This is not possible unless all the powers are zero because primes doesn't divide each other. So unless the powers are zero there is no way canceling prime power by a bunch of other prime powers. But if all the prime powers are zero then we have $a_i - c_i = 0 \iff a_i = c_i$ and $b_i - d_i = 0 \iff b_i = d_i$ for all $i \in [k]$. This means $p_i = q_i$ for all $i \in [k]$. Hence f_k is injective. Therefore f_k is injective for all $k \in \mathbb{N}$. Therefore there is an injective function for all $k > 0$ mapping $\mathbb{Q}^k$ to $\mathbb{Q}$.

Proof of $\mathbb{R}$ is Infinite-Dimensional over $\mathbb{Q}$: First we will show that any $n-$dimensional vector space over $\mathbb{Q}$ is isomorphic to $\mathbb{Q}^n$. Then if $\mathbb{R}$ is finite dimensional then $R \cong \mathbb{Q}^n$ for some $n \in \mathbb{N}$. Then we will argue that by the above theorem we have an one-one function from $f : \mathbb{R} \to \mathbb{Q}$. Then we will show this is not possible.

Lemma 6. *If V is a $n-$dimensional vector space V over $\mathbb{Q}$ then $V \cong \mathbb{Q}^n$.*

Proof: Let $B = \{b_1, \ldots, b_n\}$ be a basis of V. Now we take the standard basis $B_Q = \{v_1, \ldots, v_n\}$ for $\mathbb{Q}^n$ where v_i has 1 in the i^{th} place and $0's$ in the rest of the positions. Then we know there is unique $\theta \in L(V, \mathbb{Q}^n)$ such that $\theta(b_i) = v_i$ for all $i \in [n]$. We will show that this θ is a bijection also.

Let $x, y \in V$ such that $\theta(x) = \theta(y)$. Now $\exists\ x_i \in \mathbb{Q}$ for all $i \in [n]$ not all zero such that $x = \sum\limits_{i=1}^{n} x_i b_i$ and $\exists\ y_i \in \mathbb{Q}$ not all zero such that $y = \sum\limits_{i=1}^{n} y_i b_i$. Now

$$\theta(x) = \theta(y) \iff \theta\left(\sum_{i=1}^{n} x_i b_i\right) = \theta\left(\sum_{i=1}^{n} y_i b_i\right) \implies \sum_{i=1}^{n} x_i \theta(b_i) = \sum_{i=1}^{n} y_i \theta(b_i) \iff \sum_{i=1}^{n} x_i v_i = \sum_{i=1}^{n} y_i v_i$$

Hence we have $\sum\limits_{i=1}^{n} (x_i - y_i) v_i = 0$. Since $v_i's$ are linearly independent we have $x_i - y_i = 0 \implies x_i = y_i$ for all $i \in [n]$. Therefore $x = y$. Hence θ is injective.

Now we will prove θ is surjective. Let $w \in \mathbb{Q}^n$. Then there exists $w_1, \dots w_n \in \mathbb{Q}$ not all zero such that $w = \sum\limits_{i=1}^{n} w_i v_i$. Then consider the vector $u = \sum\limits_{i=1}^{n} w_i b_i \in V$. Then

$$\theta(u) = \theta\left(\sum_{i=1}^{n} w_i b_i\right) = \sum_{i=1}^{n} w_i \theta(b_i) = \sum_{i=1}^{n} w_i v_i = w$$

Hence for all $w \in \mathbb{Q}^n$ there exists some $u \in V$ such that $\theta(u) = w$. Therefore θ is surjective.

Therefore we get θ is a linear map which is both injective and surjective. Hence θ is bijective linear map. Therefore θ is an isomorphism between V and $\mathbb{Q}^n$. Hence $V \cong \mathbb{Q}^n$. ■

Lemma 7. *There is an injective function from $\mathbb{Q}$ to $\mathbb{Z}$.*

Proof: Let $\mathbb{Q}_+$ denote the set of all positive rational numbers. Then suppose we have an injective function from $f : \mathbb{Q}_+ \to \mathbb{N}$ then consider the function $\phi : \mathbb{Q} \to \mathbb{Z}$ such that

$$\phi(q) = \begin{cases} f(q) & \text{when } q > 0 \\ 0 & \text{when } q = 0 \\ -f(q) & \text{when } q < 0 \end{cases}$$

Then ϕ gives an injective function from $\mathbb{Q} \to \mathbb{Z}$ if f is injective.

Therefore now we will construct f. Now for any positive rational number $q = \frac{a}{b}$ we will assume a, b are in lowest form i.e. $a, b \in \mathbb{N}$, $b \neq 0$ and $gcd(a, b) = 1$. So whenever we write $q = \frac{a}{b}$ that means it is in the lowest form. Now for any $q = \frac{a}{b} \in \mathbb{Q}_+$ consider the value $a+b$. Take $d = a+b-1 \implies d \in \mathbb{N}$. We say the rational number q is in the d^{th} diagonal if $q = \frac{a}{b}$ and $a + b = d + 1$ or we say the point (a, b) is in the d^{th} diagonal if $a + b = d + 1$. Since we are only thinking of positive rational numbers there are finitely many pairs (x, y) where $x, y \in \mathbb{N}$ such that $x+y = d$. Hence there are finitely many positive rational numbers q such that the sum of the values of numerator and denominator of q in its lowest form is $d + 1$.

Now an ordered pair (x, y) is in the d^{th} diagonal if $0 \leq x \leq d$ and we can write $y = d + 1 - x$. So $(x, d + 1 - x)$ for all $x \in [d]$ are in the d^{th} diagonal. So there are d many ordered pairs in the d^{th} diagonal. Hence at most d many rationals can be on the d^{th} diagonal. So we introduce a sequence of numbers $\{T(n)\}_{n \geq 1}$ where

$$T(n) = \#\text{ordered pairs in any of the first } n \text{ diagonals} = \sum_{d=1}^{n} d = \frac{n(n+1)}{2}$$

Now $T(n)$ as a function from $\mathbb{N} \to \mathbb{N}$ is it is an injective function. So with this we define $f : \mathbb{Q}_+ \to \mathbb{N}$. For any $q \in \mathbb{Q}_+$ with $q = \frac{a}{b}$

$$f(q) = T((a + b - 1) - 1) + a$$

Basically the ordered pair (a, b) is in the $d = (a + b - 1)^{th}$ diagonal. So by $(a + b - 1) - 1$ we exhaust all the ordered pairs which are in any of the first $d-1$ diagonals. After that we go to the d^{th} diagonal and there the a^{th} point is the ordered pair (a, b). That is why we first count all the points in any of the first $(d - 1)$ diagonals and after that we count how many steps we need to go to the a^{th} point which is a.

We claim this is an injective function. So suppose $f(q) = f(p)$ for some $p, q \in \mathbb{Q}_+$, $p \neq q$. Let $q = \frac{a}{b}$ and $p = \frac{s}{t}$ in their lowest forms. We have

$$f(q) = T(a + b - 2) + a = T(s + t - 2) + c = f(p)$$

Now it will not be the case that $a+b=s+t$ because if it is then that implies (a,b) and (s,t) are in same diagonal and then $f(p)=f(q) \implies a=s \implies b=t \implies p=q$ which is not possible. So $a+b \neq s+t$. WLOG $a+b>s+t$. Then $(a+b) \geq (s+t)+1$. Now

$$T(n+1)-T(n)=\frac{(n+1)(n+2)}{2}-\frac{n(n+1)}{2}=n+1$$

Since $a+b>s+t \implies a+b-2 \geq (s+t-2)+1$ we have

$$T(a+b-2) \geq T(s+t-2)+[(s+t-2)+1]=T(s+t-2)+s+t-1$$

Therefore

$$f(p)=T(s+t-2)+s<T(s+t-2)+(s+t-1)+1<T(a+b-2)+1 \leq T(a+b-2)+a=f(q)$$

The last inequality is because $a \geq 1$. Therefore $f(p)<f(q)$ but that is not possible since we have $f(p)=f(q)$. Hence contradiction. If $p \neq q$ then $f(p) \neq f(q)$ for all $p,q \in \mathbb{Q}_+$. Hence f is injective. And therefore ϕ is also injective. Hence there is an injective function from $\mathbb{Q}$ to $\mathbb{Z}$. ■

Lemma 8. *There is an injective function from $\mathbb{Z}$ to $\mathbb{N} \cup \{0\}$.*

Proof: Consider the function $\tau : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ such that for any $k \in \mathbb{Z}$

$$\tau(k)=\begin{cases} 0 & \text{when } k=0 \\ 2k & \text{when } k>0 \\ 2|k|-1 & \text{when } k<0 \end{cases}$$

To prove this is an injective function let $\exists\ m,n \in \mathbb{Z}$, $m \neq n$ suppose $\tau(m)=\tau(n)$. Let $\tau(m)$ is even. Then $\tau(n)$ is even. Then

$$\tau(m)=2m=2n=\tau(n) \iff m=n$$

This is not possible. So suppose $\tau(m)$ is odd. Hence $\tau(n)$ is odd and $m,n<0$. So

$$\tau(m)=-2m+1=-2n+1=\tau(n) \iff m=n$$

This is not possible. But there are no other options possible. Hence contradiction. Therefore τ is an injective function. ■

Lemma 9. *There is an injective function from $\mathbb{N} \cup \{0\}$ to $\mathbb{N}$*

Proof: Consider the function $\sigma : \mathbb{N} \cup \{0\} \to \mathbb{N}$ where for any $k \in \mathbb{N} \cup \{0\}$, $\sigma(k)=k+1$. Clearly this is an injecive function since we are just shifting the value by 1. Hence σ is an injective function from $\mathbb{N} \cup \{0\}$ to $\mathbb{N}$. ■

Hence for any $n-$dimensional vector space V over $\mathbb{Q}$ there is an isomorphism ψ between V and $\mathbb{Q}^n$ by Lemma 6. Then we know that there is an injective function $f_n : \mathbb{Q}^n \to \mathbb{Q}$. Then using Lemma 7 we have that there is an injective function $\phi : \mathbb{Q} \to \mathbb{Z}$. Using Lemma 8 we have that there is an injective function $\tau : \mathbb{Z} \to \mathbb{N} \cup \{0\}$. And then using Lemma 9 we have an injective function $\sigma : \mathbb{N} \cup \{0\} \to \mathbb{N}$. Hence we have an function $\zeta_n = \sigma \circ \tau \circ \phi \circ f_n \circ \psi$ where $\zeta_n : V \to \mathbb{N}$ is an injective function. Therefore for any $n-$dimensional vector space V over $\mathbb{Q}$ there is an injective function $\zeta_n : V \to \mathbb{N}$. So if $\mathbb{R}$ is a finite dimensional vector space over $\mathbb{Q}$ then there is an injective function $\zeta : \mathbb{R} \to \mathbb{N}$. So to prove that $\mathbb{R}$ is infinite dimensional over $\mathbb{Q}$ we will prove that such an injective function can not exist.

Lemma 10. *There is no injective function $f : \mathbb{R} \to \mathbb{N}$*

Proof: Suppose there is an injective function $f : \mathbb{R} \to \mathbb{N}$. Hence we can also say there is a surjective map g from $\mathbb{N}$ to $\mathbb{R}$ because we can simply define g like this:

$$g(n) = \begin{cases} x & \text{If } \exists\ x \in \mathbb{R} \text{ such that } f(x) = n \\ 0 & \text{otherwise} \end{cases}$$

This g is a surjective function because for all $x \in \mathbb{R}$, $f(n) \in \mathbb{N}$. Hence for all $x \in \mathbb{R}$, $g(f(x)) = x$.

So now consider set of all the real numbers in the $[0, 1]$ interval with all its digits are 0 or 1. Denote this set to be S. Hence $\forall\ x \in S$, $f(x) \in \mathbb{N}$. So we can give an order $\prec$ to S in the following way: for any $x, y \in S$

$$x \prec y \iff f(x) < f(y)$$

Therefore we can say $f(S)$ forms an increasing sequence in $\mathbb{N}$. Let $\{n_k\}_{k \geq 1}$ is the sequence such that $\forall\ x \in S$, $\exists! k \in \mathbb{N}$ such that $g(n_k) = x$ and $i < j \iff n_i < n_j \iff g(n_i) \prec g(n_j)$. Now we will construct an element of $y \in S$. Let for any $x \in S$, $x(n)$ denote the n^{th} digit of x after the decimal point. So we define y like the following

$$y(k) = 1 - g(n_k)(k)$$

Certainly since $\forall\ x \in S$ for all $n \in \mathbb{N}$, $x(n) \in \{0, 1\}$ we have $\forall\ k \in \mathbb{N}$, $y(k) \in \{0, 1\}$. Therefore $y \in S$. But forall $k \in \mathbb{N}$ $g(n_k) \neq y$ since y and $g(n_k)$ differs in at least at the k^{th} digit after the decimal point. Hence $\nexists\ k \in \mathbb{N}$ such that $g(n_k) = y$. That means $\exists\ y \in S$ such that $\nexists\ n \in \mathbb{N}$ so that $g(n) = y$. Hence g is not surjective map. But we showed that if there an injective map $f : \mathbb{R} \to \mathbb{N}$ then there is an surjective map $g : \mathbb{N} \to \mathbb{R}$. Hence contradiction. There is no injective map from $\mathbb{R}$ to $\mathbb{N}$. ■

With this lemma we get there is no injective function $f : \mathbb{R} \to \mathbb{N}$. Therefore $\mathbb{R}$ can not be a finite dimensional vector space over $\mathbb{Q}$ because otherwise there will be an injective map from $\mathbb{R} \to \mathbb{N}$. Hence $\mathbb{R}$ is an infinite dimensional vector space over $\mathbb{Q}$.

■