Soham Chatterjee
Email: soham.chatterjee@tifr.res.in
Course: Mathematical Foundations of Computer Science

Assignment - 1
Dept: STCS
Date: September 6, 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:

□

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, $\text{Im}(\theta)$ is a subspace of V, and

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

(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:

(a) Define the map $\varphi : U/\ker\theta \to \text{Im}\,\theta$ 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 $\operatorname{Spec}(V)_U = \{W \subseteq V \mid W \text{ subspace of } V \text{ containing } U\}$ for any vector space V over $\mathbb{F}$. 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 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

$$\varphi\left(\psi^{-1}(S)\right) = \varphi(\{v \in V \mid v+U \in W\}) = \{\varphi(v) \mid v \in V,\ v+U \in W\} = W$$

Therefore f is bijective. Hence there is an 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 $W_1, \ldots, W_k \leq V$ be subspaces. We say that V is the internal direct sum of $W_1, \ldots, W_k$ and write $V = \bigoplus_{i=1}^{k} W_i$ if for all $v \in V$, there exists unique $w_1 \in W_1, \ldots, w_k \in W_k$ such that $v = \sum_{i=1}^{k} w_i$. The values $w_1, \ldots, w_k$ are called the projections of v onto $W_1, \ldots, W_k$ 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 $V = \mathrm{Im}(\theta) \oplus \ker(\theta)$ and for all $v \in V, \theta(v)$ is just the projection of v onto $\mathrm{Im}(\theta)$.
- Let $\theta_1, \ldots, \theta_k \in L(v)$ 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:
$$V = \bigoplus_{i=0}^{k} \mathrm{Im}\,(\theta_i)$$

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 $i \in [k]$. Hence $\sum_{i=1}^{k} W_i$ 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 $i' \in [k]$, $i' \neq i$. 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 $v \in V = \sum_{i=1}^{k}$ 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 $v = \sum_{i=1}^{k} w_i$. Therefore $V = \bigoplus_{i=1}^{k} W_i$.

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 $v = T(v) + (v - T(v))$. Certainly $T(v) \in \operatorname{Im}\theta$. 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 $v \in \operatorname{Im}\theta$ there exists $u \in V$ such that $\theta(u) = v$. Since $0 = \theta(v) = \theta \circ \theta(u) = \theta(u) = v$. 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

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

  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

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

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 $\forall\ i, j \in \{0, 1, \ldots, k\}$ 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 1. *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 $v \in |\theta\rangle_0$. 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 2. $\forall\ i \in [k]$ *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 $v \in \sum_{j\neq i} \operatorname{Im}\theta_j$, $\exists\ u_j \in V$ 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 1, Lemma 2 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 follow 2 lemmas. Then using them we will show x, y, z form a basis.

Lemma 3. $\theta(z) \neq 0$

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 $x, y = \theta(x), z = \theta(y), \theta(z) \neq 0$.

Lemma 4. *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 3 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 $q = 1$ since $gcd(p, q) = 1$. Similarly $p \mid 0$, $p \mid p^3$, $p \mid pq^2$. Hence

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

Hence both p, q are equal to 1. So 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

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

Now using (1) 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 ($ab-1,\ a+b^2-1\neq 0$): 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 4. So at least one of them is zero. Suppose exactly one of them zero.

Case 2 ($ab-1=0,\ a+b^2-1\neq 0$): Then $(a+b^2-1)y=0 \implies y=0$ then we have $\theta(z)=0$ which contradicts Lemma 3.

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

Case 4 ($ab-1=a+b^2-1=0$): 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 $s=1$. Again

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

Hence we have $a=1$. But 1 is not a 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:

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

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

Therefore we get product of powers of prime numbers is 1. Hence for each prime the power of the prime has to be 0 because otherwise this is not possible. 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 $\log p_1, \ldots, \log p_{n+1}$ is linearly independent over $\mathbb{Q}$. But $\dim \mathbb{R} = n$ over $\mathbb{Q}$. 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 $(q_1, \ldots, q_k) \in \mathbb{Q}$.

□