MATH2040A Homework 3 **Reference Solutions**

Compulsory Part 1

1.6.12. Let u, v and w be distinct vectors of a vector space V. Show that if $\{u, v, w\}$ is a basis for V, then $\{u + v + w, v + w, w\}$ is also a basis for V.

Solution: Since $\{u, v, w\}$ is a basis, it is easy to see that u + v + w, v + w, w are distinct, so dim $(V) = |\{u, v, w\}| = 3 =$ $|\{u+v+w, v+w, w\}|$. So, to show that $\{u+v+w, v+w, w\}$ is a basis, it suffices to show only one of linear independence and that it spans the whole space. Here we show only the linear independence.

Let $a, b, c \in \mathbb{F}$ be such that a(u+v+w) + b(v+w) + cw = 0. Then 0 = a(u+v+w) + b(v+w) + cw = au + (a+b)v + (a+b+c)w. As $\{u, v, w\}$ is a basis, it is linearly independence. So a = a + b = a + b + c = 0, which implies a = b = c = 0. Hence $\{u+v+w, v+w, w\}$ is linearly independent. By Corollary 2 of Theorem 1.10 in textbook, $\{u+v+w, v+w, w\}$ is a basis for V.

1.6.15. Find a basis for W, the set of all $n \times n$ matrices having trace equal to zero. What is the dimension of W?

Solution: For all $i, j \in \{1, ..., n\}$ let $E^{ij} \in M_{n \times n}(\mathbb{F})$ be the matrix that the (i, j)-entry is one and all other entries are zero. Let $S = \{ E^{ij} : i, j \in \{1, ..., n\}, i \neq j \} \cup \{ -E^{11} + E^{ii} : i \in \{2, ..., n\} \}$. It is easy to see that $\{ E^{ij} : i, j \in \{1, ..., n\} \}$ is a basis of $M_{n \times n}(\mathbb{F})$ and that $|S| = (n^2 - n) + (n - 1) = n^2 - 1$.

If $n = 1, S = \emptyset$, which is a basis for $W = \{ (0) \}$, which is of dimension |S| = 0. In the remaining proof we will assume that n > 1.

We show that S is linearly independent and spans W.

- (a) For $i, j \in \{1, ..., n\}$ with $(i, j) \neq (1, 1)$ let $a_{ij} \in \mathbb{R}$ be such that $\sum_{\substack{i, j \in \{1, ..., n\}\\ i \neq j}} a_{ij} E^{ij} + \sum_{k=2}^{n} a_{kk} (-E^{11} + E^{kk}) = 0.$ Then $\sum_{\substack{i, j \in \{1, ..., n\}\\ (j, j) \neq (1, 1)}} a_{ij} E^{ij} + \sum_{k=2}^{n} a_{kk} E^{kk} \sum_{k=2}^{n} a_{kk} E^{11} = 0.$ Since $\{E^{ij} : i, j \in \{1, ..., n\}\}$ is a basis, it is linearly

independent and so $a_{ij} = 0$ for all $i, j \in \{1, \ldots, n\}$ with $(i, j) \neq (1, 1)$ and $a_{kk} = 0$ for all $k \in \{2, \ldots, n\}$. Hence S is linearly independent.

(b) It is easy to see that $S \subseteq W$ and so Span $(S) \subseteq W$. We now show the reverse direction.

Let $A \in W$. Then $A \in M_{n \times n}(\mathbb{F})$ and tr A = 0. As $\left\{ E^{ij} : i, j \in \{1, \dots, n\} \right\}$ is a basis of $M_{n \times n}(\mathbb{F})$, we may assume that $A = \sum_{i,j \in \{1,\dots,n\}} a_{ij} E^{ij}$. Then $0 = \text{tr } A = \sum_{k=1}^{n} a_{kk}, -a_{11} = \sum_{k=2}^{n} a_{kk}$. This implies that $A = \sum_{i,j \in \{1,\dots,n\}} a_{ij} E^{ij} = \sum_{i,j \in \{1,\dots,n\}} a_{ij} E^{ij} + \sum_{k=2}^{n} a_{kk} (E^{kk} - E^{11}) \in \text{Span}(S)$.

$$i \neq j$$

As A is arbitrary, $W \subseteq \text{Span}(S)$ and so S spans W.

As S is linearly independent and spans W, S is a basis of W. The dimension of W is then $\dim(W) = |S| = n^2 - 1$.

Note

Another common choice of basis is $\{ E^{ij} : i, j \in \{ 1, ..., n \}, i \neq j \} \cup \{ -E^{i-1,i-1} + E^{ii} : i \in \{ 2, ..., n \} \}.$

1.6.23. Let v_1, \ldots, v_k, v be vectors in a vector space V, and define $W_1 = \text{Span}(\{v_1, \ldots, v_k\})$, and $W_2 = \text{Span}(\{v_1, \ldots, v_k, v\})$. (a) Find necessary and sufficient conditions on v such that $\dim(W_1) = \dim(W_2)$

- (b) State and prove a relationship involving $\dim(W_1)$ and $\dim(W_2)$ in the case that $\dim(W_1) \neq \dim(W_2)$.

Solution:

(a) Since $\{v_1, \ldots, v_k\} \subseteq \{v_1, \ldots, v_k, v\}$, we have $W_1 = \text{Span}(\{v_1, \ldots, v_k\}) \subseteq \text{Span}(\{v_1, \ldots, v_k, v\}) = W_2$. Also, as W_2 is spanned by a finite set $\{v_1, \ldots, v_k, v\}$, $\dim(W_2) \leq |\{v_1, \ldots, v_k, v\}| \leq k + 1 < \infty$. Hence, by Theorem 1.11, $\dim(W_1) = \dim(W_2)$ if and only if $W_1 = W_2$.

Suppose $W_1 = W_2$. Then $v \in W_2 = W_1 = \text{Span}(\{v_1, \dots, v_k\})$. We now show that this condition is also sufficient. Suppose now $v \in \text{Span}(\{v_1, \dots, v_k\})$. Then for all $x \in \{v_1, \dots, v_k, v\}$, $x \in W_1$, so $W_2 = \text{Span}(\{v_1, \dots, v_k, v\}) \subseteq W_1$. As we already have $W_1 \subseteq W_2$, this implies that $W_1 = W_2$.

So dim (W_1) = dim (W_2) if and only if $v \in$ Span $(\{v_1, \ldots, v_k\}) = W_1$.

(b) $\dim(W_1) + 1 = \dim(W_2)$ when $\dim(W_1) \neq \dim(W_2)$.

Suppose dim $(W_1) \neq$ dim (W_2) . Then by the previous part, $v \notin W_1$. Let β be a basis of W_1 . Then β is linearly independent, and $v \notin$ Span (β) . In particular, $v \notin \beta$. By Theorem 1.7, $\beta \cup \{v\}$ is linearly independent.

For all $x \in \{v_1, \ldots, v_k, v\}$, $x \in \text{Span}(\beta \cup \{v\})$, so $W_2 = \text{Span}(\{v_1, \ldots, v_k, v\}) \subseteq \text{Span}(\beta \cup \{v\})$. As $\beta \subseteq W_1 \subseteq W_2$ and $v \in W_2$, we have $\beta \cup \{v\} \subseteq W_2$ and so $\text{Span}(\beta \cup \{v\}) \subseteq W_2$. This two imply that $\beta \cup \{v\}$ spans W_2 and so is a basis of W_2 . Hence $\dim(W_2) = |\beta \cup \{v\}| = |\beta| + 1 = \dim(W_1) + 1$.

Note

We cannot use Theorem 1.7 on $\{v_1, \ldots, v_k\}$ because we do not know if it is linearly independent or not.

For part (b), although $\dim(W_1) < \dim(W_2)$ and $\dim(W_1) \neq \dim(W_2)$ also such conditions, we will not accept these as answers since they are too trivial. Similar for $\dim(W_1)$, $\dim(W_2)$, and any other combinations of their sum / difference being (positive) integer.

1.6.26. For a fixed $a \in \mathbb{R}$ determine the dimension of the subspace of $\mathsf{P}_n(\mathbb{R})$ defined by $\{f \in \mathsf{P}_n(\mathbb{R}) : f(a) = 0\}$.

Solution: Denote $\{ f \in \mathsf{P}_n(\mathbb{R}) : f(a) = 0 \}$ by V. Let $S = \{ (x-a)x^k : k \in \{ 0, ..., n-1 \} \} \subseteq \mathsf{P}(\mathbb{R})$. Then $S \subseteq \mathsf{P}_n(\mathbb{R})$ and f(a) = 0 for all $f \in S$, so $S \subseteq V$. We now show that S is a basis of V. Trivially we have $\operatorname{Span}(S) \subseteq V$. Let $f \in V$. Then $f \in \mathsf{P}_n(\mathbb{R})$ and f(a) = 0. By factor theorem, there exists a polynomial

Trivially we have $\operatorname{Span}(S) \subseteq V$. Let $f \in V$. Then $f \in \mathsf{P}_n(\mathbb{R})$ and f(a) = 0. By factor theorem, there exists a polynomial $g \in \mathsf{P}(\mathbb{R})$ such that f = (x - a)g. As $n \ge \deg f = 1 + \deg g$, we have $\deg g \le n - 1$. This implies that $g \in \mathsf{P}_{n-1}(\mathbb{R})$ is a linear combination of the basis $\{x^k : k \in \{0, \ldots, n-1\}\}$, so $g = \sum_{k=0}^{n-1} a_k x^k$ for some $a_k \in \mathbb{R}, k \in \{0, \ldots, n-1\}$. Hence, $f = (x - a)g = \sum_{k=0}^{n-1} a_k(x - a)x^k \in \operatorname{Span}(S)$. Since f is arbitrary, $V = \operatorname{Span}(S)$.

We now show that S is linearly independent. This would implies that S is a basis for V. Let $a_k \in \mathbb{R}$ for $k \in \{0, \ldots, n-1\}$ be such that $\sum_{k=0}^{n-1} a_k(x-a)x^k = 0$. Then $-a_0a + \sum_{k=1}^{n-1} (a_{k-1} - aa_k)x^k + a_{n-1}x^n = 0$. Since $\{x^k : k \in \{0, \ldots, n\}\}$ is linearly independent, we have that $-a_0a = a_{n-1} = 0$ and $a_{k-1} - aa_k = 0$ for all $k \in \{1, \ldots, n-1\}$. This implies that $a_k = 0$ for all $k \in \{0, \ldots, n-1\}$, so S is linearly independent.

Note

Another common choices of basis are $\{(x-a)^k : k \in \{1, ..., n\}\}$ and $\{x^k - a^k : k \in \{1, ..., n\}\}$. Also, we adapt the convention that $\deg 0 = -\infty$ so that $\deg(fg) = \deg f + \deg g$ holds for all $f, g \in \mathsf{P}(\mathbb{R})$.

1.6.30. Let

$$V = M_{2 \times 2}(\mathbb{F}), \quad W_1 = \left\{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \in V : a, b, c \in \mathbb{F} \right\}$$

and

$$W_2 = \left\{ \begin{array}{cc} 0 & a \\ -a & b \end{array} \right\} \in V : \ a, b \in \mathbb{F} \left\}$$

Prove that W_1 and W_2 are subspaces of V, and find the dimensions of $W_1, W_2, W_1 + W_2$ and $W_1 \cap W_2$.

Solution:

Although in this homework we do not deduct points if you have given only the basis without providing a proof, please note that *in principle* you **still** need to justify that you set indeed forms a basis as claimed. If for example you do not give appropriate justifications on your sets during tests and exams, then we *may* mark your proof as incomplete/incorrect.

2.1.14. Let V and W be vector spaces and $T:V \to W$ be linear.

- (a) Prove that T is one-to-one if and only if T carries linearly independent subsets of V onto linearly independent subsets of W
- (b) Suppose that T is one-to-one and that S is a subset of V. Prove that S is linearly independent if and only if T(S) is linearly independent

(c) Suppose $\beta = \{ v_1, \dots, v_n \}$ is a basis for V and T is one-to-one and onto. Prove that $T(\beta) = \{ T(v_1), \dots, T(v_n) \}$ is a basis for W.

Solution:

(a) Suppose T is one-to-one. Let $S \subseteq V$ be linearly independent, and $\{T(v_1), \ldots, T(v_n)\} \subseteq T(S)$ be a finite subset of T(S) for some $n \in \mathbb{N}$ with $v_1, \ldots, v_n \in S$. Let $a_1, \ldots, a_n \in \mathbb{F}$ be such that $\sum_{i=1}^n a_i T(v_i) = 0$. Then $T(\sum_{i=1}^n a_i v_i) = 0$. As T is one-to-one, $\sum_{i=1}^n a_i v_i = 0$. As S is linearly independent, so is $\{v_1, \ldots, v_n\}$, hence $a_i = 0$ for all $i \in \{1, \ldots, n\}$. This implies that $\{T(v_1), \ldots, T(v_n)\}$ is linearly independent. As $\{T(v_1), \ldots, T(v_n)\}$ is arbitrary, T(S) is linearly independent.

Suppose T maps linearly independent subsets of V to linearly independent subsets of W. Let $v \in V \setminus \{0\}$. Then $\{v\}$ is linearly independent, so $\{Tv\} = T\{v\}$ is linearly independent. This implies that $Tv \neq 0$ and so $v \notin \ker T$. Hence $\ker T = \{0\}$, and so T is one-to-one.

Therefore T is one-to-one if and only if T maps linearly independent subsets of V to linearly independent subsets of W.

(b) Suppose S is linearly independent. Then by the previous part, T(S) is linearly independent since T is one-to-one.

Suppose T(S) is linearly independent. Let $\{v_1, \ldots, v_n\} \subseteq S$ be a finite subset of S with $n \in \mathbb{N}$, and $a_1, \ldots, a_n \in \mathbb{F}$ be such that $\sum_{i=1}^n a_i v_i = 0$. Then $\sum_{i=1}^n a_i T(v_i) = T(\sum_{i=1}^n a_i v_i) = 0$. By the linear independence of T(S), $a_i = 0$ for all $i \in \{1, \ldots, n\}$. This implies that $\{v_1, \ldots, v_n\}$ is linearly independent. As $\{v_1, \ldots, v_n\}$ is arbitrary, S is linearly independent.

Therefore T(S) is linearly independent if and only if S is linearly independent.

(c) Since β is a basis, it is linearly independent. As T is one-to-one, by part (a) $T(\beta)$ is linearly independent.

Let $w \in W$. As T is onto, there exists $v \in V$ such that Tv = w. As β is a basis for V, there exists $a_1, \ldots, a_n \in \mathbb{F}$ such that $v = \sum_{i=1}^n a_i v_i$. So $w = Tv = T(\sum_{i=1}^n a_i v_i) = \sum_{i=1}^n a_i T(v_i) \in \text{Span}(T(\beta))$. As w is arbitrary, $W \subseteq \text{Span}(T(\beta))$. Trivially, we also have $\text{Span}(T(\beta)) \subseteq W$ as $T(\beta) \subseteq W$ and so $W = \text{Span}(T(\beta))$.

Since $T(\beta)$ is linearly independent and spans W, $T(\beta)$ is a basis for W.

Note

In the first two parts we have to take finite subsets of the original sets because we do not know if they are finite or not.

2.1.17. Let V and W be finite-dimensional vector spaces and $T: V \to W$ be linear.

- (a) Prove that if $\dim(V) < \dim(W)$, then T cannot be onto.
- (b) Prove that if $\dim(V) > \dim(W)$, then T cannot be one-to-one.

Solution:

- (a) Suppose $\dim(V) < \dim(W)$. Then by Dimension Theorem, $\dim(W) > \dim(V) = \operatorname{nullity} T + \operatorname{rank} T \ge 0 + \dim(\mathsf{R}(T))$. This implies that $\dim(W) \neq \dim(\mathsf{R}(T))$ and so $W \neq \mathsf{R}(T)$. Hence T is not onto.
- (b) Suppose $\dim(V) > \dim(W)$. Then by Dimension Theorem, $\dim(W) < \dim(V) = \operatorname{nullity} T + \operatorname{rank} T \le \dim(\mathsf{N}(T)) + \dim(W)$. This implies that $\dim(\mathsf{N}(T)) \neq 0$. So $\mathsf{N}(T) \neq \{0\}$. Hence T is not one-to-one.

2.1.21. Let V be the vector space of sequences. Define the functions $T, U: V \to V$ by

 $T(a_1,...) = (a_2, a_3,...)$ and $U(a_1,...) = (0, a_1,...)$

- (a) Prove that T and U are linear
- (b) Prove that T is onto, but not one-to-one
- (c) Prove that U is one-to-one, but not onto

Solution:

(a) Let $x = (x_1, ...), y = (y_1, ...) \in V, c \in \mathbb{F}$. Then

1. $T(cx + y) = T(c(x_1, \ldots) + (y_1, \ldots)) = T(cx_1 + y_1, cx_2 + y_2, \ldots) = (cx_2 + y_2, \ldots) = c(x_2, \ldots) + (y_2, \ldots) = cT(x_1, x_2, \ldots) + T(y_1, y_2, \ldots) = cT(x) + T(y)$

2. $U(cx + y) = U(c(x_1, \ldots) + (y_1, \ldots)) = U(cx_1 + y_1, cx_2 + y_2, \ldots) = (0, cx_1 + y_1, \ldots) = c(0, x_1, \ldots) + (0, y_1, \ldots) = cU(x_1, x_2, \ldots) + U(y_1, y_2, \ldots) = cU(x) + U(y)$

As x, y, c are arbitrary, T, U are linear.

- (b) i. Let $(x_1, x_2, \ldots) \in V$. Then $(0, x_1, x_2, \ldots) \in V$ and $(x_1, x_2, \ldots) = T(0, x_1, x_2, \ldots) \in \mathsf{R}(T)$. As $(x_1, x_2, \ldots) \in V$ is arbitrary, T is onto.
 - ii. Let $x = (1, 0, 0, ...) \in V$ be the sequence such that the first entry is 1 and every entry else is 0. Then T(x) = (0, 0, ...) = 0 = T(0) but $x \neq 0$. This implies that T is not one-to-one.
- (c) i. Let $(x_1, x_2, \ldots) \in V$ be such that $U(x_1, x_2, \ldots) = 0$. Then $(0, x_1, x_2, \ldots) = U(x_1, x_2, \ldots) = (0, 0, 0, \ldots)$ and so $x_i = 0$ for all $i \in \mathbb{Z}^+$, $(x_1, x_2, \ldots) = 0$. As (x_1, x_2, \ldots) is arbitrary, U is one-to-one.
 - ii. Let $x = (1, 0, 0, ...) \in V$ be the sequence such that the first entry is 1 and every entry else is 0. Then for $y = (y_1, y_2, ...) \in V$, $U(y) = (0, y_1, y_2, ...) \neq (1, 0, 0, ...) = x$. This implies that $x \notin \mathsf{R}(U)$. Hence U is not onto.
- 2.1.22. Let $T : \mathbb{R}^3 \to \mathbb{R}$ be linear. Show that there exists scalars a, b, c such that T(x, y, z) = ax + by + cz for all $(x, y, z) \in \mathbb{R}^3$. Can you generalize this results for $T : \mathbb{F}^n \to \mathbb{F}$? State and prove an analogous result for $T : \mathbb{F}^n \to \mathbb{F}^m$.

Solution:

(a) Let $a = T(1,0,0), b = T(0,1,0), c = T(0,0,1) \in \mathbb{R}$. We show that T(x,y,z) = ax + by + cz for all $(x,y,z) \in \mathbb{R}^3$. For all $(x,y,z) \in \mathbb{R}^3$, we have (x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1) and so T(x,y,z) = T(x(1,0,0) + y(0,1,0) + z(0,0,1)) = xT(1,0,0) + yT(0,1,0) + zT(0,0,1) = ax + by + cz.

(b) For linear map $T: \mathbb{F}^n \to \mathbb{F}$, there exists $a_1, \ldots, a_n \in \mathbb{F}$ such that $T(x_1, \ldots, x_n) = \sum_{i=1}^n a_i x_i$ for all $(x_1, \ldots, x_n) \in \mathbb{F}^n$.

(c) For linear map $T : \mathbb{F}^n \to \mathbb{F}^m$, there exists $a_{ij} \in \mathbb{F}$ for $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$ such that $T(x_1, \ldots, x_n) = \left(\sum_{j=1}^n a_{1j}x_j, \ldots, \sum_{j=1}^n a_{mj}x_j\right)$ for all $(x_1, \ldots, x_n) \in \mathbb{F}^n$.

For all $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$ let $a_{ij} \in \mathbb{F}$ be such that $Te_j = (a_{1j}, \ldots, a_{mj})$ with $e_j \in \mathbb{F}^n$ be the vector that the *j*th component is 1 and all other components are 0. Then for all $(x_1, \ldots, x_n) \in \mathbb{F}^n$, $(x_1, \ldots, x_n) = \sum_{j=1}^n x_j e_j$ and so $T(x_1, \ldots, x_n) = T\left(\sum_{j=1}^n x_j e_j\right) = \sum_{j=1}^n x_j Te_j = \sum_{j=1}^n x_j (a_{1j}, \ldots, a_{mj}) = \left(\sum_{j=1}^n a_{1j} x_j, \ldots, \sum_{j=1}^n a_{mj} x_j\right).$

Note

See also Theorem 2.6.

2.1.35. Let V be a finite-dimensional vector space and $T: V \to V$ be linear.

- (a) Suppose $V = \mathsf{R}(T) + \mathsf{N}(T)$. Prove that $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.
- (b) Suppose $\mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$. Prove that $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.

Solution: We present here two proofs that use different approaches. Other approaches are also welcomed.

The first proof utilizes the result of Question 1.6.29, or Theorem 2.43 in Axler's *Linear Algebra Done Right* (in Edition 3), namely:

Lemma. Let U, W be subspaces of a finite-dimensional vector space V. Then $\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

- (a) Since V is finite-dimensional, by dimension theorem and the result of Question 1.6.29, we have $\dim(\mathsf{R}(T)) + \dim(\mathsf{N}(T)) = \operatorname{rank} T + \operatorname{nullity} T = \dim(V) = \dim(\mathsf{R}(T) + \mathsf{N}(T)) = \dim(\mathsf{R}(T)) + \dim(\mathsf{N}(T)) \dim(\mathsf{R}(T) \cap \mathsf{N}(T))$. As all quantities are finite, we have $\dim(\mathsf{R}(T) \cap \mathsf{N}(T)) = 0$ and so $\mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$. This implies that $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.
- (b) Since V is finite-dimensional, by dimension theorem and the result of Question 1.6.29, we have $\dim(\mathsf{R}(T) + \mathsf{N}(T)) = \dim(\mathsf{R}(T)) + \dim(\mathsf{N}(T)) \dim(\mathsf{R}(T) \cap \mathsf{N}(T)) = \operatorname{rank} T + \operatorname{nullity} T \dim(\{0\}) = \dim(V)$. As $V \supseteq \mathsf{R}(T) + \mathsf{N}(T)$, we have $V = \mathsf{R}(T) + \mathsf{N}(T)$, which implies that $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.

The second proof does not use Question 1.6.29 and is more convoluted, but it gives more insights on the subspaces.

(a) In view of the definition of direct sum, it suffices to show that $\mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$.

Let $v \in \mathsf{R}(T) \cap \mathsf{N}(T)$. Then there exists $w \in V$ such that Tw = v and Tv = 0, so $T^2w = Tv = 0$, $w \in \mathsf{N}(T^2)$. If we have $\mathsf{N}(T^2) = \mathsf{N}(T)$, then this would implies that $w \in \mathsf{N}(T)$ and so v = Tw = 0. Since v is arbitrary, we would then have $\mathsf{R}(T) \cap \mathsf{N}(T) \subseteq \{0\}$. As the reverse direction is trivial, we would have $\mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$.

So it suffices to show that $\mathsf{N}(T^2) = \mathsf{N}(T)$. For each $x \in \mathsf{N}(T)$ we have Tx = 0 and so $T^2x = T(Tx) = T(0) = 0$, $x \in \mathsf{N}(T^2)$, so $\mathsf{N}(T) \subseteq \mathsf{N}(T^2)$. Since V is finite-dimensional, by dimension theorem we have $\dim(\mathsf{R}(T)) + \dim(\mathsf{N}(T)) = \dim(\mathsf{R}(T^2)) + \dim(\mathsf{N}(T^2))$, so it suffices to show that $\dim(\mathsf{R}(T)) = \dim(\mathsf{R}(T^2)) < \infty$, which would imply that $\dim(\mathsf{N}(T)) = \dim(\mathsf{N}(T^2))$ and hence give that desired relation.

Let $v \in \mathsf{R}(T)$. Then for some $w \in V$, Tw = v. Since $V = \mathsf{R}(T) + \mathsf{N}(T)$, there exists $x \in V$ such that w = Tx + (w - Tx) with $w - Tx \in \mathsf{N}(T)$, $v - T^2x = Tw - T^2x = T(w - Tx) = 0$, $v = T^2x \in \mathsf{R}(T^2)$. As v is arbitrary, $\mathsf{R}(T) \subseteq \mathsf{R}(T^2)$. Trivially, for each $v \in \mathsf{R}(T^2)$ there also exists $w \in V$ such that $v = T^2w = T(Tw) \in \mathsf{R}(T)$. So $\mathsf{R}(T^2) = \mathsf{R}(T)$. In particular, $\dim(\mathsf{R}(T^2)) = \dim(\mathsf{R}(T)) < \infty$.

Therefore $\mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$ and so $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.

(b) In view of the definition of direct sum, it suffices to show that $\mathsf{R}(T) + \mathsf{N}(T) = V$.

Let $v \in V$. Then $Tv \in \mathsf{R}(T)$. If we have $\mathsf{R}(T) = \mathsf{R}(T^2)$, then there would exist $w \in V$ such that $Tv = T^2w = T(Tw)$ and so $Tw \in \mathsf{R}(T)$ and $T(v - Tw) = Tv - T^2w = 0$, $v - Tw \in \mathsf{N}(T)$, which would imply that $v = Tw + (v - Tw) \in \mathsf{R}(T) + \mathsf{N}(T)$. Since v is arbitrary, we would have $V \subseteq \mathsf{R}(T) + \mathsf{N}(T)$. As the reverse direction is trivial, we would have $V = \mathsf{R}(T) + \mathsf{N}(T)$.

So it suffices to show that $\mathsf{R}(T) = \mathsf{R}(T^2)$. For each $x \in \mathsf{R}(T^2)$ there exists $y \in V$ such that $x = T^2 y = T(Ty) \in \mathsf{R}(T)$, so $\mathsf{R}(T^2) \subseteq \mathsf{R}(T)$. Since V is finite-dimensional, by dimension theorem $\dim(\mathsf{R}(T)) + \dim(\mathsf{N}(T)) = \dim(\mathsf{N}(T^2)) + \dim(\mathsf{N}(T^2))$, so it suffices to show that $\dim(\mathsf{N}(T)) = \dim(\mathsf{N}(T^2)) < \infty$, which would imply that $\dim(\mathsf{R}(T)) = \dim(\mathsf{R}(T^2))$ and hence give the desired relation.

Let $v \in \mathsf{N}(T^2)$. Then we have $T(Tv) = T^2v = 0$, so $Tv \in \mathsf{N}(T)$. Trivially we also have $Tv \in \mathsf{R}(T)$, which implies that $Tv \in \mathsf{R}(T) \cap \mathsf{N}(T) = \{0\}$ and so Tv = 0, $v \in \mathsf{N}(T)$. As v is arbitrary, $\mathsf{N}(T^2) \subseteq \mathsf{N}(T)$. Trivially, for each $v \in \mathsf{N}(T)$ we also have Tv = 0 and so $T^2v = 0$, $v \in \mathsf{N}(T^2)$. So $\mathsf{N}(T) = \mathsf{N}(T^2)$. In particular, $\dim(\mathsf{N}(T)) = \dim(\mathsf{N}(T^2)) < \infty$.

Therefore $\mathsf{R}(T) + \mathsf{N}(T) = V$ and so $V = \mathsf{R}(T) \oplus \mathsf{N}(T)$.

Note

Notice the symmetry in both proofs, and how the finite dimension assumption is used besides for the dimension theorem.

You can also use a cardinality argument on the bases and their intersections and unions to avoid invoking the lemma directly, but the proof would just be a simplified version to that of Question 1.6.29, which we refer to the reference solution given in the Optional part below.

For the second proof, you can also show further relations regarding the iterated ranges and nullspaces.

2 Optional Part

1.6.4. Do the polynomials $x^3 - 2x^2 + 1$, $4x^2 - x + 3$, and 3x - 2 generate $\mathsf{P}_3(\mathbb{R})$? Justify your answer.

Solution: No.

Since dim($\mathsf{P}_3(\mathbb{R})$) = 4, by replacement theorem (and its corollary), a spanning set must have at least 4 vectors. Since $\{x^3 - 2x^2 + 1, 4x^2 - x + 3, 3x - 2\}$ has only 3 < 4 vectors, it does not generate $\mathsf{P}_3(\mathbb{R})$. In particular, it does not generate the constant polynomial 1.

1.6.20. Let V be a vector space having dimension n, and let S be a subset of V that generates V.

(a) Prove that there is a subset of S that is a basis for V.

(b) Prove that S contains at least n vectors.

Solution:

(a) Since $\dim(V) = n < \infty$, there exists a (finite) basis $\beta = \{e_1, \ldots, e_n\}$ of V. Since S spans V, every vector in β is a linear combination of finitely many vectors in S. Since β is a finite set, (after a renaming) there exists $m \in \mathbb{N}, v_1, \ldots, v_m \in S$ such that $e_i \in \text{Span}(\{v_1, \ldots, v_m\})$ for all $i \in \{1, \ldots, n\}$. Then for $S' = \{v_1, \ldots, v_m\}$, $V = \text{Span}(\beta) \subseteq \text{Span}(S') \subseteq V$, so $S' \subseteq S$ generates V.

Let $S_0 = \emptyset$. For each $i \in \{1, \ldots, m\}$ define iteratively that

$$S_i = \begin{cases} S_{i-1} & \text{if } v_i \in \text{Span}(S_{i-1}) \\ S_{i-1} \cup \{v_i\} & \text{if } v_i \notin \text{Span}(S_{i-1}) \end{cases}$$

Then for each $i \in \{1, \ldots, m\}$, $S_i \subseteq S'$, $v_i \in \text{Span}(S_i)$ and $\text{Span}(S_{i-1}) \subseteq \text{Span}(S_i)$, hence $\text{Span}(S_m) = \text{Span}(S') = V$. Also, as $S_0 = \emptyset$ is linearly independent, using the definition of S_i we can show by induction that S_i is linearly independent for all $i \in \{0, \ldots, m\}$.

Therefore, S_m is a linearly independent subset of $S' \subseteq S$ that spans V, so $S_m \subseteq S$ is a basis of V.

In particular, S contains a basis for V.

(b) Define S_m as above. As S_m is a basis, $|S_m| = n$. So $|S| \ge |S_m| = n$.

Note

Part (a) is done by constructing a basis from S. Since S could be uncountable (e.g. the whole of V), it would be tricky to construct a basis by enumerating its elements. Hence in the above proof we extract a countable (even finite) subset S' that has the same span and work on this subset instead.

- 1.6.29. (a) Prove that if W_1 and W_2 are finite-dimensional subspaces of a vector space V, then the subspace $W_1 + W_2$ is a finite-dimensional, and $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) \dim(W_1 \cap W_2)$.
 - (b) Let W_1 and W_2 be finite-dimensional subspaces of a vector space V, and let $V = W_1 + W_2$. Deduce that V is the direct sum of W_1 and W_2 if and only if dim $(V) = \dim(W_1) + \dim(W_2)$.

Solution:

(a) We first show that $W_1 + W_2$ is finite-dimensional.

Let β_1, β_2 be bases of W_1, W_2 respectively. Then $\dim(W_1) = |\beta_1| < \infty$, $\dim(W_2) = |\beta_2| < \infty$, and β_1, β_2 span W_1, W_2 respectively. So $W_1 + W_2 = \text{Span}(\beta_1) + \text{Span}(\beta_2) = \text{Span}(\beta_1 \cup \beta_2)$ and hence $\dim(W_1 + W_2) \le |\beta_1 \cup \beta_2|$. Since $|\beta_1 \cup \beta_2| \le |\beta_1| + |\beta_2| < \infty$, $W_1 + W_2$ is finite-dimensional.

Let β be a basis of $W_1 \cap W_2$, which is a subspace of $W_1 + W_2$ and so is also finite-dimensional. By Corollary 2 of the replacement theorem, β can be extended to (finite) bases γ_1, γ_2 of W_1, W_2 respectively, so that $\beta \subseteq \gamma_1 \cap \gamma_2$.

As the bases are all finite, we may let $\beta = \{e_1, \ldots, e_n\}, \gamma_1 \setminus \beta = \{f_1, \ldots, f_m\}, \gamma_2 \setminus \beta = \{g_1, \ldots, g_p\}$ with $n, m, p \in \mathbb{N}$ (with a zero index meaning empty set). If $f_i = g_j$ for some i, j, as $f_i \in W_1$ and $g_j \in W_2$ we would have $f_i = g_j \in W_1 \cap W_2 = \text{Span}(\gamma)$ and so γ_1 and γ_2 would be linearly dependent. This implies that $\gamma_1 \setminus \beta$ and $\gamma_2 \setminus \beta$ are disjoint, and so $\beta = \gamma_1 \cap \gamma_2$ and $\gamma_1 \cup \gamma_2 = \{e_1, \ldots, e_n, f_1, \ldots, f_m, g_1, \ldots, g_p\}$.

We now show that $\gamma_1 \cup \gamma_2$ is a basis of $W_1 + W_2$. Since γ_1, γ_2 are bases of W_1, W_2 receptively, we have $\text{Span}(\gamma_1 \cup \gamma_2) = \text{Span}(\gamma_1) + \text{Span}(\gamma_2) = W_1 + W_2$.

It remains to show that $\gamma_1 \cup \gamma_2$ is linearly independent. Let $a_1, \ldots, a_n, b_1, \ldots, b_m, c_1, \ldots, c_p \in \mathbb{F}$ be such that

$$\sum_{i=1}^{n} a_i e_i + \sum_{j=1}^{m} b_j f_j + \sum_{k=1}^{p} c_k g_k = 0$$

Then

$$\sum_{i=1}^{n} a_i e_i + \sum_{j=1}^{m} b_j f_j = -\sum_{k=1}^{p} c_k g_k \in \text{Span}(\gamma_1) \cap \text{Span}(\gamma_2) = W_1 \cap W_2$$

 So

$$\sum_{i=1}^{n} a_i e_i + \sum_{j=1}^{m} b_j f_j = \sum_{i=1}^{n} d_i e_i$$

for some $d_1, \ldots, d_n \in \mathbb{F}$ and thus

$$\sum_{i=1}^{n} (a_i - d_i)e_i + \sum_{j=1}^{m} b_j f_j = 0$$

As γ_1 is a basis, it is linearly independent and so $a_i - d_i = 0$ and $b_j = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$. So

$$\sum_{i=1}^{n} a_i e_i + \sum_{k=1}^{p} c_k g_k = 0$$

As γ_2 is a basis, it is linearly independent and so $a_i = c_j = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, p\}$. This implies that $\gamma_1 \cup \gamma_2$ is linearly independent.

Therefore $\gamma_1 \cup \gamma_2$ is a basis of $W_1 + W_2$. This implies that $\dim(W_1 + W_2) = |\gamma_1 \cup \gamma_2| = n + m + p = (n+m) + (n+p) - n = |\gamma_1| + |\gamma_2| - |\beta| = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2).$

(b) By the previous part, $\dim(V) = \dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$. So $V = W_1 \oplus W_2$ if and only if $W_1 \cap W_2 = \{0\}$ if and only if $\dim(W_1 \cap W_2) = 0$ if and only if $\dim(V) = \dim(W_1) + \dim(W_2)$.

Note

See also the inclusion–exclusion principle in set theory. Try generalizing this to 3 (or more) subspaces.

1.6.31. Let W_1 and W_2 be subspaces of a vector space V having dimensions m and n, respectively, where $m \ge n$.

- (a) Prove that $\dim(W_1 \cap W_2) \leq n$
- (b) Prove that $\dim(W_1 + W_2) \le m + n$

Solution:

(a) As $W_1 \cap W_2 \subseteq W_2$, we have $\dim(W_1 \cap W_2) \leq \dim(W_2) = n$.

- (b) By Question 1.6.29, $\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) \dim(W_1 + W_2) \le \dim(W_1) + \dim(W_2) = m + n$.
- 1.6.34. (a) Prove that W_1 is any subspace of a finite-dimensional vector space V, then there exists a subspace W_2 of V such that $V = W_1 \oplus W_2$
 - (b) Let $V = \mathbb{R}^2$ and $W_1 = \{ (a_1, 0) : a_1 \in \mathbb{R} \}$. Give examples of two different subspaces W_2 and W'_2 such that $V = W_1 \oplus W_2$ and $V = W_1 \oplus W'_2$

Solution:

(a) Let β be a basis of W_1 . Since V is finite-dimensional, W is also finite-dimensional, and so we may assume that $\beta = \{ w_1, \ldots, w_n \}$ for some $n \in \mathbb{N}$. By the corollary of replacement theorem, β can be extended to a (finite) basis $\gamma \supseteq \beta$ of V. Let $\gamma \setminus \beta = \{ v_1, \ldots, v_m \}$ for some $m \in \mathbb{N}$. Let $W_2 = \text{Span}(\gamma \setminus \beta)$. It is easy to see that W_2 is also a subspaces of V.

We now show that W_2 has the desired property.

- i. By the property of basis, we have $V = \text{Span}(\gamma) = \text{Span}(\beta \cup (\gamma \setminus \beta)) = \text{Span}(\beta) + \text{Span}(\gamma \setminus \beta) = W_1 + W_2$.
- ii. It is easy to see that $\{0\} \subseteq W_1 \cap W_2$. Let $v \in W_1 \cap W_2$. Then there exists scalars $a_1, \ldots, a_n, b_1, \ldots, b_m \in \mathbb{F}$ such that $v = \sum_{i=1}^n a_i w_i = \sum_{j=1}^m b_j v_j$. Then $\sum_{i=1}^n a_i w_i - \sum_{j=1}^m b_j v_j = 0$. As $\gamma = \{w_1, \ldots, w_n, v_1, \ldots, v_m\}$ is a basis, it is linearly independent and so $a_i = b_j = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$. So $v = \sum_{i=1}^n a_i w_i = 0$. This implies that $W_1 \cap W_2 \subseteq \{0\}$ and so $W_1 \cap W_2 = \{0\}$.

By definition of direct sum, we have that $V = W_1 \oplus W_2$.

(b) Let $W_2 = \text{Span}(\{(0,1)\})$ and $W'_2 = \text{Span}(\{(1,1)\})$. We shall omit the detailed proof here but it is easy to see that

- 1. $W_2 \neq W'_2$
- 2. $W_1 \cap W_2 = W_1 \cap W_2' = \{(0,0)\}$
- 3. $W_1 + W_2 = W_1 + W_2' = \mathbb{R}^2 = V$
- So $V = W_1 \oplus W_2 = W_1 \oplus W'_2$.

2.1.12. Is there a linear transformation $T: \mathbb{R}^3 \to \mathbb{R}^2$ such that T(1,0,3) = (1,1) and T(-2,0,-6) = (2,1)?

Solution: No.

Suppose there exists one such linear map T. Then $(2,1) = T(-2,0,-6) = T(-2 \cdot (1,0,3)) = -2T(1,0,3) = -2(1,1) = (-2,-2)$. Contradiction arises. So no such linear map exists.

2.1.26. Assume that $T: V \to V$ is the projection on W_1 along W_2 .

- (a) Prove that T is linear and $W_1 = \{ x \in V : T(x) = x \}$
- (b) Prove that $W_1 = \mathsf{R}(T)$ and $W_2 = \mathsf{N}(T)$.
- (c) Describe T if $W_1 = V$.
- (d) Describe T if W_1 is the zero subspace

Solution:

(a) Since V = W₁ ⊕ W₂, for each vector x ∈ V the decomposition x = x₁ + x₂ with x₁ ∈ W₁, x₂ ∈ W₂ is unique. So the map T is well-defined. Furthermore, by the definition of T, for each x ∈ V the decomposition x = Tx + (x - Tx) conforms to the space decomposition V = W₁ ⊕ W₂.
Let x, y ∈ V and α ∈ 𝔽. As V = W₁ ⊕ W₂, by the property of direct sum there exists (unique) x₁, y₁ ∈ W₁ and

 $x_2, y_2 \in W_2$ such that $x = x_1 + x_2$ and $y = y_1 + y_2$. By the definition of projection, $Tx = x_1$ and $Ty = y_1$. Since W_1, W_2 are subspaces, $x + y = (x_1 + y_1) + (x_2 + y_2)$ and $\alpha x = \alpha x_1 + \alpha x_2$ with $x_1 + y_1, \alpha x_1 \in W_1$ and $x_2 + y_2, \alpha x_2 \in W_2$, so $T(x + y) = x_1 + y_1 = Tx + Ty$ and $T(\alpha x) = \alpha x_1 = \alpha Tx$. As x, y, α are arbitrary, T is linear.

Let $w \in W_1$. Then w = w + 0 with $w \in W_1$ and $0 \in W_2$. So Tw = w, $w \in \{x \in V : Tx = x\}$.

Let $x \in V$ be such that Tx = x. Let $x = x_1 + x_2$ with $x_1 \in W_1, x_2 \in W_2$. Then $x = Tx = x_1 \in W_1$. As x is arbitrary, $\{x \in V : Tx = x\} \subseteq W_1$.

Hence $W_1 = \{ x \in V : Tx = x \}.$

- (b) i. By the previous part, we have $W_1 = \{ x \in V : Tx = x \} \subseteq \mathsf{R}(T)$. Let $x \in \mathsf{R}(T)$. Then for some $y \in V$, Ty = x. Then y = Ty + (y - Ty) = x + (y - x) satisfies $y - x \in W_2$ and $x \in W_1$. As x is arbitrary, $\mathsf{R}(T) \subseteq W_1$. Hence $W_1 = \mathsf{R}(T)$.
 - ii. Let $x \in N(T)$. Then Tx = 0. So x = Tx + (x Tx) = 0 + x satisfies $0 \in W_1$ and $x \in W_2$. As x is arbitrary, $N(T) \subseteq W_2$.
 - Let $x \in W_2$. Then x = 0 + x with $0 \in W_1$ and $x \in W_2$. So by definition of T, we have Tx = 0, $x \in \mathbb{N}(T)$. As x is arbitrary, $W_2 \subseteq \mathbb{N}(T)$. Hence $W_2 = \mathbb{N}(T)$.
- (c) Suppose $W_1 = V$. By part (a), $V = W_1 = \{x \in V : Tx = x\}$, so T is the identity map on $W_1 = V$ and so is the identity map.
- (d) Suppose $W_1 = \{0\}$. By part (b), $\{0\} = W_1 = \mathsf{R}(T)$, so Tx = 0 for all $x \in V$ and so T is the zero map.

2.1.27. Suppose that W is a subspace of a finite-dimensional vector space V.

- (a) Prove that there exists a subspace W' and a function $T: V \to V$ such that T is a projection on W along W'
- (b) Give an example of a subspace W of a vector space V such that there are two projections on W along two (distinct) subspaces.

Solution:

- (a) To construct such subspace W' and such map $T: V \to V$, it suffices to construct W' as a subspace of V such that $V = W \oplus W'$. Then the map T can be constructed in the canonical way (i.e. as defined for Question 2.1.26). However, by the result of Question 1.6.34(a), such subspace W' can always be constructed. So the desired subspace W' and the desired map $T: V \to V$ always exists.
- (b) Define V, W_1, W_2, W'_2 as in Question 1.6.34(b). Then $V = W_1 \oplus W_2 = W_1 \oplus W'_2$. Let T, T' be the canonical projection map on W_1 along W_2 and W'_2 respectively. Then T, T' are the desired maps.

Note

As we can see from the above answer, specifying a projection map is *basically* the same as specifying a pair of direct summands (in a specific order).

2.1.31. Suppose that $V = \mathsf{R}(T) \oplus W$ and W is T-invariant.

(a) Prove that $W \subseteq \mathsf{N}(T)$

- (b) Show that if V is finite-dimensional, then $W = \mathsf{N}(T)$
- (c) Show by example that the conclusion of (b) is not necessarily true if V is not finite-dimensional

Solution:

- (a) Since $V = \mathsf{R}(T) \oplus W$, we have that $W \cap \mathsf{R}(T) = \{0\}$. Since $0 \in T(W)$, $T(W) \subseteq W$ and $T(W) \subseteq \mathsf{R}(T)$, we have $\{0\} \subseteq T(W) \subseteq W \cap \mathsf{R}(T) = \{0\}$ and so $T(W) = \{0\}$. This implies that $W \subseteq \mathsf{N}(T)$.
- (b) By dimension theorem and the result of Question 1.6.29, we have rank T + nullity $T = \dim(V) = \dim(\mathbb{R}(T)) + \dim(W) \dim(\mathbb{R}(T) \cap W) = \operatorname{rank} T + \dim(W) \dim(\{0\}) = \operatorname{rank} T + \dim(W)$. Since rank $T \leq \dim(V) < \infty$, we have $\dim(\mathbb{N}(T)) = \operatorname{nullity} T = \dim(W)$.

By the previous part, we have $W \subseteq \mathsf{N}(T)$, so $W = \mathsf{N}(T)$.

(c) Let V be the real sequence space, $T: V \to V$ be the left shift operator, and $W = \{0\}$ be the zero subspace of V. It is easy to see that $\mathsf{R}(T) = V$, W is T-invariant, and $V = \mathsf{R}(T) \oplus W$, but $\mathsf{N}(T) = \{(a, 0, 0, \ldots) : a \in \mathbb{R}\} \neq W$.

2.1.32. Suppose that W is T-invariant. Prove that $N(T_W) = N(T) \cap W$ and $R(T_W) = T(W)$.

Solution:

- (a) Let $v \in \mathsf{N}(T_W)$. Then $v \in W$ and $T_W(v) = 0$. By definition of T_W , we have that $T(v) = T_W(v) = 0$, so $v \in \mathsf{N}(T)$. So $v \in \mathsf{N}(T) \cap W$. As v is arbitrary, $\mathsf{N}(T_W) \subseteq \mathsf{N}(T) \cap W$. Let $w \in \mathsf{N}(T) \cap W$. Then $w \in \mathsf{N}(T)$ and $w \in W$. So T(w) = 0. As $w \in W$, $T_W(w)$ is well-defined and $T_W(w) = T(w) = 0$, so $w \in \mathsf{N}(T_W)$. As w is arbitrary, $\mathsf{N}(T) \cap W \subseteq \mathsf{N}(T_W)$. Therefore $\mathsf{N}(T_W) = \mathsf{N}(T) \cap W$.
- (b) Let $v \in \mathsf{R}(T_W)$. Then for some $w \in W$, $T_W(w) = v$. By definition of T_W , we have $v = T_W(w) = T(w) \in T(W)$. As v is arbitrary, $\mathsf{R}(T_W) \subseteq T(W)$. Let $v \in T(W)$. Then for some $w \in W$, v = T(w). As $w \in W$, $T_W(w)$ is well-defined and $v = T(w) = T_W(w) \in \mathsf{R}(T_W)$. As v is arbitrary, $T(W) \subseteq \mathsf{R}(T_W)$. Therefore $\mathsf{R}(T_W) = T(W)$.

3 Appendix

In general field, you cannot replace " $a_1, \ldots a_n \in \mathbb{F}$ not all zero" with " $a_1^2 + \ldots + a_n^2 \neq 0$ ". For example, consider $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$, the field with two elements which we will call 0, 1 where 0 is the zero element. Then $1 \neq 0$ but $1^2 + 1^2 = 1 + 1 = 0$.