Chapter 1: Spaces

Juan Patricio Carrizales Torres

Sep 29, 2022

1 Fields

In Linear Algebra, we will be working with numbers from any type of class/set. Hence, to simplify things and make them more general, we will introduce the idea of fields. A **field** is a set of objects (including numbers) called **scalars** with operations of addition and multiplication that fulfill the following rules (let α and β be scalars):

(a) **Addition**

  (a) commutatitivity, $\alpha + \beta = \beta + \alpha$.

  (b) associativity, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

  (c) additive identity, there is a unique scalar 0 such that for every scalar α, $\alpha + 0 = \alpha$.

  (d) additive inverse, for each scalar α there is a unique scalar $-\alpha$ such that $\alpha + (-\alpha) = 0$.

(b) **Multiplication**

  (a) commutativity, $\alpha\beta = \beta\alpha$.

  (b) associativity, $\gamma(\alpha\beta) = (\gamma\alpha)\beta$.

  (c) multiplicative identity, there is a unique nonzero scalar 1 for every scalar α such that $1\alpha = \alpha$.

  (d) multiplicative inverse, for every nonzero scalar β, there is a unique β^{-1} such that $\beta\beta^{-1} = 1$.

(c) **Linearity**

  (a) Multiplication is distributive over addition, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

For instance, the class of real numbers and the class of complex numbers are fields.

1.1 Excercises

Problem 1. Almost all the laws of elementary arithmetic are consequences of the axioms defining a field. Prove, in particular, that if $\mathcal{F}$ is a field, and if α, β and γ belong to $\mathcal{F}$, then the following relations hold.

(a) $0 + \alpha = \alpha$

Proof. Due to the commutativity property of addition, $\alpha = \alpha + 0 = 0 + \alpha$. □

(b) If $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$.

Proof. Due to the additive inverse, associativity and commutativity, $\alpha + \beta + (-\alpha) = \alpha + (\beta + (-\alpha)) = (\alpha + (-\alpha)) + \beta = \beta = \gamma$. □

(c) $\alpha + (\beta - \alpha) = \beta$.

Proof. Just like in (b),

$$\begin{aligned} \alpha + (\beta + (-\alpha)) &= \alpha + (-\alpha + \beta) \\ &= (\alpha + (-\alpha)) + \beta = 0 + \beta \\ &= \beta. \end{aligned}$$

□

(d) $\alpha \cdot 0 = 0 \cdot \alpha = 0$. (In this case, the dot indicates multiplication).

Proof. Note that

$$\begin{aligned} 0 \cdot \alpha + (-0 \cdot \alpha) = 0 &= (0 + 0)\alpha + (-0 \cdot \alpha) \\ &= 0 \cdot \alpha + (0 \cdot \alpha + (-0 \cdot \alpha)) = 0 \cdot \alpha \\ &= \alpha \cdot 0 \end{aligned}$$

□

(e) $(-1)\alpha = -\alpha$

Proof. Observe that

$$\begin{aligned} \alpha + (-\alpha) = 0 &= 0\alpha \\ &= (1 - 1)\alpha = \alpha + (-1)\alpha. \end{aligned}$$

By (b), $-\alpha = (-1)\alpha$. □

(f) $(-\alpha)(-\beta) = \alpha\beta$.

Proof. By (e), $(-\alpha)(-\beta) = ((-1)\alpha)((-1)\beta)$. Then,

$$\begin{aligned}((-1)\alpha)((-1)\beta) &= (-1)(\alpha((-1)\beta)) \\ &= (-1)((\alpha(-1))\beta) = (-1)(((-1)\alpha)\beta) \\ &= ((-1)((-1)\alpha))\beta = (((-1)(-1))\alpha)\beta \\ &= (1\alpha)\beta = \alpha\beta\end{aligned}$$

□

(g) $\alpha\beta = 0 \implies \alpha = 0$ or $\beta = 0$.

Proof. Let $\alpha\beta = 0$. Note that either $\alpha = 0$ or $\alpha \neq 0$. In the first case, the result is true. In the case of the latter, there is some α^{-1} and so $\alpha^{-1}\alpha\beta = 1\beta = \alpha^{-1}0 = 0$. □

Problem 2. (a) Is the set of all positive integers a field? (In familiar systems, such as the integers, we shall almost always use the ordinary operations of addition and multiplication. On the rare occasions when we depart from this convention, we shall give ample warning. As for "positive", by that word we mean, here and elsewhere in this book, "greater than or equal to zero". If 0 is to be excluded, we shall say "strictly positive".)

Solution It is not a field. Although the commutativity, associativity and linearity of closed addition and multiplication is maintained, there is and additive identitiy 0 and the multiplicative identity 1 is present in this set, there are no additive inverses and multiplicative inverses.

(b) What about the set of integers?

Solution It is still not a field. It just needs some type of identity multiplicative.

(c) Can the answers to these questions be changed by re-defining addition or multiplication (or both)?

Solution We can re-define addition and multiplication so that there are multiplicative identities for every positive integers. Consider some integer α. Let's mantain all known properties but make this small change

$$\alpha^2 = \sum^{\alpha} \alpha = 1.$$

Every integer is its own multiplicative inverse.

Problem 2. Let m be an integer, $m \geq 2$, and let Z_m be the set of all positive integers less than m, $Z_m = \{0, 1, \ldots, m-1\}$. If α and β are in Z_m, let $\alpha + \beta$ be the least positive remainder obtained by dividing the (ordinary) sum of α and β by m, and, similarly, let $\alpha\beta$ be the least remainder obtained by dividing the (ordinary) product of α and β by m. (Example: if $m = 12$, then $3 + 11 = 2$ and $3 \cdot 11 = 9$.)

(a) Prove that Z_m is a field if and only if m is a prime.

Proof. Let m be a prime number. Note that addition and multiplication are both closed, commutative, associative and linear in the set of positive integers and so their least remainder when divided by m is in $\mathbb{Z}_m$ (recall the equivalence classes in integers modulo m). Since $m \geq 2$, there is the additive identity 0 and additive multiplicative 1. Also, 0 is its own additive inverse. Now consider some nonzero $\alpha \in Z_m$, then $m > m - \alpha > 0$ and $m - \alpha \in Z_m$. Since $\alpha + (m - \alpha) = m = 0$, it follows that $m - \alpha$ is the unique additive inverse of α.
Now, we show for any nonzero $x \in Z_m$ that $x \cdot Z_m = Z_m$ (multiplication of all elements of Z_m by α) to prove the existence of some multiplicative inverse. Consider some nonzero $x \in Z_m$ and so $x = m - \beta$ where $\beta \in \{1, \ldots, m-1\}$. Note that there are only m possible remainders when dividing a positive integer by m and all are contained in Z_m. Hence, the only way $x \cdot Z_m \neq Z_m$ is when $|x \cdot Z_m| < |Z_m|$, namely, when there are distinct $y, z \in Z_m$ such that both $x \cdot y$ and $x \cdot z$ have the same remainder when divided by m. We show this is not possible when m is a prime integer.
Consider two distinct $y, z \in Z_m$ and so $y = m - \alpha$ and $z = m - \gamma$ for $\alpha, \gamma \in \{1, \ldots, m\}$. Observe that

$$|(m-\beta)(m-\alpha) - (m-\beta)(m-\gamma)| = |(m-\beta)(\gamma-\alpha)|\,.$$

Since $y \neq z$, it follows that $\gamma \neq \alpha$ and so $\gamma - \alpha \neq 0$. Furthermore, $|\gamma - \alpha| < m$. Thus, $(m-\beta)(\gamma-\alpha)$ is the multiplication of two numbers that are not multiples of m and so $|(m-\beta)(\gamma-\alpha)|$ is not a multiple of m since m is a prime number. Therefore, $m \nmid |y - z|$ and so y and z do not have equal remainder when divided by m. Thus, $x \cdot Z_m$ for any $x \in Z_m$ and so there is some $y \in Z_m$ such that $x \cdot y = 1$ (multiplicative inverse). This argument can be used to show that the multiplicative inverse for any nonzero $\alpha \in Z_m$ is unique.

For the converse, assume that Z_m is a field. By **Problem 1**, for any elements $\alpha, \beta \in Z_m$, $\alpha\beta = 0$ if and only if at least one of them is 0. This implies that all possible multiplications between the nonzero positive integers lower than m are not multiples of m. Thus, m is a factorization of itself times 1, m must be a prime number. □

(b) What is -1 in Z_5

Solution Let the operations be extended to any integers, not just the ones inside Z_5. We know that -5 is a multiple of 5 and we must add -4 to -1 to get to -5. See this as some type of remainder, just as we need to add -2 to 2 to get to 0. Hence, -1 in Z_5 is 4.

(c) What is $\frac{1}{3}$ in Z_7?

Solution It is not defined, since there is no integer in $\alpha \in Z_7$ such that $\frac{1}{3} - \alpha$ is divisible by 7.

Problem 5. Let $Q(\sqrt{2})$ be the set of all real numbers of the form $\alpha + \beta\sqrt{2}$, where α and β are rational.

(a) Is $Q(\sqrt{2})$ a field?

Proof. Yes, it is a field. Note that $Q(\sqrt{2}) \subseteq \mathbb{R}$ and so the properties of commutativity, associativity and linearity of multiplication and addition are present. Also, $\alpha+\beta\sqrt{2}, -\alpha-\beta\sqrt{2} \in Q(\sqrt{2})$. Furthermore, $1+0\sqrt{2}, 0+0\sqrt{2} \in Q(\sqrt{2})$. We now show that addition and multiplication are closed. Consider some $\alpha + \beta\sqrt{2}$ and $\gamma + \epsilon\sqrt{2}$, where $\alpha, \beta, \gamma, \epsilon \in \mathbb{Q}$. Observe that

$$\left(\alpha + \beta\sqrt{2}\right) + \left(\gamma + \epsilon\sqrt{2}\right) = (\alpha + \gamma) + (\beta + \epsilon)\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$$

and

$$\begin{aligned}\left(\alpha + \beta\sqrt{2}\right)\left(\gamma + \epsilon\sqrt{2}\right) &= \alpha\gamma + \alpha\epsilon\sqrt{2} + \gamma\beta\sqrt{2} + 2\beta\epsilon \\ &= (\alpha\gamma + 2\beta\epsilon) + (\alpha\epsilon + \gamma\beta)\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)\end{aligned}$$

since $\mathbb{Q}$ is closed under multiplication and addition.

We just have to show that every nonzero element of $\mathbb{Q}\left(\sqrt{2}\right)$ has a unique inverse in $\mathbb{Q}\left(\sqrt{2}\right)$. Consider some $\alpha + \beta\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. If $\alpha = 0$ or $\beta = 0$, then $\frac{1}{2\beta}\sqrt{2}$ and $\frac{1}{\alpha}$ are their inverses,respectively. If $\alpha, \beta \neq 0$, then $\frac{\alpha}{\alpha^2-2\beta^2} - \frac{\beta}{\alpha^2-2\beta^2}\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ is its inverse (Note that $\alpha^2 - 2\beta^2 = 0$ if and only if $|\alpha| = \sqrt{2}|\beta| \notin \mathbb{Q}$).
Actually, we can use the same argument to show that $\mathbb{Q}\left(\sqrt{c}\right)$ is a field for any $c \in \mathbb{Q}$. □

(b) What if α and β are required to be integers?

Proof. Then it is not a field since not all members have a multiplicative inverse. For instance, consider $\alpha + 0\sqrt{2} \in \mathbb{Z}\left(\sqrt{2}\right)$ for some integer $|\alpha| > 1$. Since $\alpha \in \mathbb{Z}$ its inverse is $\frac{1}{\alpha}$, however it is not an integer. □

Problem 6. (a) Does the set of all polynomials with integer coefficitents form a field?

Proof. No. The unique multiplicative identity is the polynomial $g(x) = 1$. We show that there is an infinity of polynomials in our set without inverse multiplicative. Consider some polynomial $p(x) = 0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n$ where $n \in \mathbb{N}$. Multiplying it by any other polynomial $s(x) = b_0 + b_1x^1 + \cdots + b_kx^k$ for $k \in \mathbb{N}$, we get that

$$\begin{aligned}p(x)s(x) &= \left(0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n\right)\left(b_0 + b_1x^1 + \cdots + b_kx^k\right) \\ &= 0\left(b_0 + b_1x^1 + \cdots + b_kx^k\right) + a_1x^1\left(b_0 + b_1x^1 + \cdots + b_kx^k\right) \\ &\quad + \cdots + a_nx^n\left(b_0 + b_1x^1 + \cdots + b_kx^k\right).\end{aligned}$$

The polynomial $p(x)s(x)$ is not a constant and so it can not be the multiplicative identity. □

(b) What if the coefficients are allowed to be real numbers?

Solution The previous argument can still be used to show that it is not a field.

Problem 7. Let $\mathcal{F}$ be the set of all (ordered) pairs (α, β) of real numbers.

(a) If addition and multiplication are defined by

$$(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta)$$

and

$$(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \beta\delta),$$

does $\mathcal{F}$ become a field?

Proof. No, it is not a field. Some conditions may be fulfilled. For insatnce, since $\mathbb{R}$ is a field and the elements of the j'th place are added and multiplied, its easy to see that addition and multiplication is closed, commutative, associative and linear. However, since ther is no multiplicative inverse for 0, it follows that there is no ordered tuple (α, β) such that $(1, 0)(\alpha, \beta) = (1, 1)$. Hence, it is a nonzero element without multiplicative inverse. □

(b) If addition and multiplication are defined by

$$(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta)$$

and

$$(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma),$$

is $\mathcal{F}$ a field then?

Proof. Yes, it is a field. Both addition and multiplication are closed since we are defining our operations as their application to the real elements inside the ordered tuples. Furthermore, as in the previous excercise, its easy to see why addition is associative and commutative. Also, for any scalar (α, β), $(\alpha, \beta) + (0, 0) = (\alpha, \beta)$ and $(\alpha, \beta) + (-\alpha, -\beta) = (0, 0)$. We show the required properties of multiplication. Consider the scalars $(\alpha, \beta), (\gamma, \delta)$ and (ϵ, ζ)

1. Commutativity:

$$\begin{aligned}(\alpha, \beta)(\gamma, \delta) &= (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma) \\ &= (\gamma\alpha - \delta\beta, \delta\alpha + \gamma\beta) = (\gamma, \delta)(\alpha, \beta)\end{aligned}$$

2. Associativity:

$$\begin{aligned}[(\alpha,\beta)(\gamma,\delta)]\,(\varepsilon,\zeta) &= (\alpha\gamma-\beta\delta,\alpha\delta+\beta\gamma)(\varepsilon,\zeta)\\ &= \alpha\gamma\varepsilon-(\beta\delta\varepsilon+\alpha\delta\zeta+\beta\gamma\zeta)\\ &= (\alpha,\beta)(\gamma\varepsilon-\delta\zeta,\gamma\zeta+\delta\varepsilon) = (\alpha,\beta)\,[(\gamma,\delta)(\varepsilon,\zeta)]\end{aligned}$$

3. Multiplicative identity:
   Consider the scalar $(1,0)$. Then,

$$(\alpha,\beta)(1,0) = (\alpha-0,0+\beta) = (\alpha,\beta)$$

   and so $(1,0)$ is the multiplicative identitity.

4. Multiplicative inverse:

   If either $\alpha=0$ or $\beta=0$, then the multplicative inverses are $(0,-1/\beta)$ and $(1/\alpha,0)$, respectively. On the other hand, if both $\alpha,\beta\neq 0$, then

$$\left(\frac{\alpha}{\alpha^2+\beta^2},-\frac{\beta}{\alpha^2+\beta^2}\right)$$

   is the miltiplicative inverse.

5. Linearity:

$$\begin{aligned}(\alpha,\beta)\,[(\gamma,\delta)+(\epsilon,\zeta)] &= (\alpha,\beta)(\gamma+\epsilon,\delta+\zeta)\\ &= (\alpha(\gamma+\epsilon)-\beta(\delta+\zeta),\alpha(\delta+\zeta)+\beta(\gamma+\epsilon))\\ &= ((\alpha\gamma-\beta\delta)+(\alpha\epsilon-\beta\zeta),(\alpha\delta+\beta\gamma)+(\alpha\zeta+\beta\epsilon))\\ &= (\alpha,\beta)(\gamma,\delta)+(\alpha,\beta)(\epsilon,\zeta)\end{aligned}$$

□

(c) What happens (in both the preceding cases) if we consider ordered pairs of complex numbers instead?

Proof. Then (a) is still not a field and (b) is a field. This is so, since the properties of operations of real numbers are maintained for the complex field. Also, $0,1\in\mathbb{C}$. □

2 Vector Space

Just like fields, we have another type of set called the **Vector Space** with elements called **vectors** over some field $\mathcal{F}$. This set comes with two operations of addition and multiplication with the following properties:

(a) ADDITION: For any vectors x and y there is a vector $x+y$ in the space (closed under addition).

1. commutativity, $x + y = y + x$.
2. associativity, $(x + y) + z = x + (y + z)$.
3. additive identity, there is a unique vector 0 such that for every vector x, $x+0 = x$.
4. additive inverse, for every vector x, there is a unique vector $-x$ such that $x + (-x) = 0$.

   As a comment, note that this are the same properties that addition has in the elemnts of a field. This is a similarity that both vector spaces and fields share: addition over their elements with these properties.

(b) MULTIPLICATION: This is not a multiplication between vectors but a scalar multplication, namely, for any vector x and scalar α there is a vector αx in the space (closed under scalar multiplication).

1. associativity, $\alpha(\beta x) = (\alpha\beta)x$.
2. $1x = x$ for every vector x

   Observe that multiplication is not defined between vectors but between a scalar and a vector. That's why multiplication can be interpreted as the application of operators on the elements of the vector space.

(c) CONNECTION: Just like in the properties of linearity for fields, vector spaces have properties that connect both structures of vector addition and scalar addition (field) in scalar multiplication (vector space).

1. Scalar multiplication is distributive with respect to scalar addition, $(\alpha + \beta)x = \alpha x + \beta x$
2. Scalar multiplication is distributive with respect to vector addition, $\alpha(x + y) = \alpha x + \alpha y$.

It's easy to see that any field $\mathcal{F}$ over itself is a vector space. Furthermore, we can extende this generalization to $\mathcal{F}^n$ for any $n \in \mathbb{N}$ by mathematical induction, if we define addition and scalar multiplication as the field addition and multiplication between the elements of the ordered n-tuples. For instance,

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$$

and

$$\gamma(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\gamma\alpha_1, \gamma\alpha_2, \ldots, \gamma\alpha_n).$$

Then, $\mathbb{R}^3$ over $\mathbb{R}$ is a real vector space and $\mathbb{C}$ over $\mathbb{C}$ is a complex vector space.

Another interesting question is related to the minimum of elements a field and a vector space must have. The smallest field is $\mathcal{F} = \{0, 1\}$ and the smallest vector space is $V = \{0\}$, since these are the only necessary elements in the properties. The other properties only discuss the characteristics of the operation.

Problem 1. Prove that if x and y are vectors and if α is a scalar, then the following relations hold.

(a) $0 + x = x$.

Proof. We now that $x + 0 = x$. Since addition is commutative, $0 + x = x + 0 = x$. □

(b) $-0 = 0$.

Proof. The additive inverse of 0 is -0. Then, $0 + (-0) = 0$. However, we know that 0 is the additive identity. Thus, $0 + (-0) = -0 = 0$. The additive inverse of the additive identity is itself. This makes sense since the addition of 0 with another nonzero vector gives the nonzero vector. □

(c) $\alpha \cdot 0 = 0$.

Proof. Let's check whether multiplying 0 by some scalar α changes its properties. Consider any x and so αx is a vector. Then,

$$\begin{aligned} \alpha \cdot 0 + \alpha \cdot x &= \alpha \cdot (0 + x) \\ &= \alpha \cdot x. \end{aligned}$$

Thus, $\alpha \cdot 0 = 0$ (We can add the additive inverse of αx to both sides). Thishas to do with the uniqueness of the additive identity. □

(d) $0 \cdot x = 0$. (The symbol 0 on the left of scalar multiplication denotes a scalar, on the right it denotes a vector).

Proof. Simply apply the distributive property with respect to scalar addition, namely,

$$\begin{aligned} 0 \cdot x + \alpha \cdot x &= (0 + \alpha) \cdot x \\ &= \alpha \cdot x. \end{aligned}$$

Then, $0 \cdot x$. Thus, the scalar 0 can be seen as some operator that neutralizes the vector. □

(e) If $\alpha x = 0$, then either $\alpha = 0$ or $x = 0$ (or both).

Proof. Suppose that $\alpha = 0$. Then, the result is true. On the other hand, assume that $\alpha \neq 0$. Consider some nonzero vector c. Then,

$$\begin{aligned} \alpha \cdot x + \alpha \cdot c &= \alpha \cdot (x + c) \\ &= \alpha \cdot c. \end{aligned}$$

Then, Multiplying both sides by the inverse of α, $x + c = c$. Thus, $x = 0$. □

(f) $-x = (-1)x$.

Proof. Note that

$$\begin{aligned} x + (-x) &= 0 \\ &= (1 + (-1)) \cdot x \\ &= x + (-1) \cdot x. \end{aligned}$$

Then, $-x = (-1) \cdot x$. □

(g) $y + (x - y) = x$. (Here $x - y = x + (-y)$.)

Proof. Note that

$$\begin{aligned} y + (x - y) &= y + (-y + x) \\ &= (y - y) + x = 0 + x. \end{aligned}$$

□

Problem 2. If p is a prime, then $\mathbb{Z}_p^n$ is a vector space over $\mathbb{Z}_p$; how many vectors are there in this vector space?

Solution Because a vector space is closed under addition and scalar multiplication we consider the cardinality of $\mathbb{Z}_p^n$. We know that $\mathbb{Z}_p$ contains p elements and there is a bijection from $\mathbb{Z}_p^n$ to all possible permutations with n elements of $\mathbb{Z}_p$. Hence, the cardinality of the vector space in question is p^n.

Problem 3. Let $\mathcal{V}$ be the set of all (ordered) pairs of real numbers. If $x = (\xi_1, \xi_2)$ and $y = (\eta_1, \eta_2)$ are elements of $\mathcal{V}$, write

$$\begin{aligned} x + y &= (\xi_1 + \eta_1, \xi_2 + \eta_2) \\ \alpha x &= (\alpha \xi_1, 0) \\ 0 &= (0, 0) \\ -x &= (-\xi_1, -\xi_2). \end{aligned}$$

Is $\mathcal{V}$ a vector space with respect to these definitions of linear operations? Why?

Solution The set $\mathcal{V}$ over $\mathbb{R}$ is not a vector space with respect to thes definitions of operations. Note that the scalar 1 is no longer a mutltiplicative identity with respect to scalar multiplication because

$$1x = (1 \cdot \xi_1, 0) \neq (\xi_1, \xi_2) = x$$

Problem 4. Sometimes a subset of a vector space is itself a vector space (with respect to the linear operations already given). Consider, for example, the vector space $\mathbb{C}^3$ and the subsets $\mathcal{V}$ of $\mathbb{C}^3$ consisting of those vectors (ξ_1, ξ_2, ξ_3) for which

(a) ξ_1 is real,

(b) $\xi_1 = 0$.

(c) either $\xi_1 = 0$ or $\xi_2 = 0$,

(d) $\xi_1 + \xi_2 = 0$,

(e) $\xi_1 + \xi_2 = 1$.

In which of these cases is $\mathcal{V}$ a vector space?

Solution Note that the set $\mathcal{V} \subseteq \mathbb{C}^3$ over $\mathbb{C}$ has the same linear operations with their required properties for a vector space. Hence, we must only check if $\mathcal{V}$ is closed under these linear operations, each vector has its respective inverse and $0 \in \mathcal{V}$ to conclude whether it is a vector space or not.
Then, (a), (c) and (e) are not vector spaces since

$$\begin{aligned}
\alpha \cdot (\xi_1, \xi_2, \xi_3) = (\alpha\xi_1, \alpha\xi_2, \alpha\xi_3) \notin \mathcal{V}, \text{ for } \alpha \in \mathbb{C}/\mathbb{R} \text{ (not closed)}, \\
(\xi_1, 0, \xi_3) + (0, \gamma_2, \gamma_3) = (\xi_1, \gamma_2, \gamma_3 + \xi_3) \notin \mathcal{V}, \text{ for } \xi_1, \gamma_2 \neq 0 \text{ (not closed) and} \\
(\xi_1, \xi_2, \xi_3) + (\gamma_1, \gamma_2, \gamma_3) = (\xi_1 + \gamma_1, \xi_2 + \gamma_2, \xi_3 + \gamma_3) \notin \mathcal{V}, \text{ because } \xi_1 + \gamma_1 + \xi_2 + \gamma_2 = 2 \\
\text{(not closed)},
\end{aligned}$$

respectively.
On the other hand, $(0, 0, 0) \in \mathcal{V}_b, \mathcal{V}_d$, where $\mathcal{V}_x$ is the subset of case x. Furtheremore, for $\mathcal{V}_b$,

$$\begin{aligned}
(0, \xi_2, \xi_3), (0, -\xi_2, -\xi_3) \in \mathcal{V}_b \\
\alpha \cdot (0, \xi_2, \xi_3) = (\alpha 0, \alpha\xi_2, \alpha\xi_3) \in \mathcal{V}_b \text{ and} \\
(0, \xi_2, \xi_3) + (0, \gamma_2, \gamma_3) = (0 + 0, \xi_2 + \gamma_2, \xi_3 + \gamma_3) \in \mathcal{V}_b.
\end{aligned}$$

In the case of $\mathcal{V}_d$, note that each vector $(\xi_1, \xi_2, \xi_3) = (\xi_1, -\xi_1, \xi_3)$ due to the uniqueness of the additive inverse in the field $\mathbb{C}$, and so

$$\begin{aligned}
(\xi_1, -\xi_1, \xi_3), (-\xi_1, \xi_1, -\xi_3) \in \mathcal{V}_d \\
\alpha \cdot (\xi_1, -\xi_1, \xi_3) = (\alpha\xi_1, -\alpha\xi_1, \alpha\xi_3) \in \mathcal{V}_b \text{ and} \\
(\xi_1, -\xi_1, \xi_3) + (\gamma_1, -\gamma_1, \gamma_3) = (\xi_1 + \gamma_1, -(\xi_1 + \gamma_1), \xi_3 + \gamma_3) \in \mathcal{V}_b.
\end{aligned}$$

Problem 5. Consider the vector space $\mathcal{P}$ and the subsets $\mathcal{V}$ of $\mathcal{P}$ consisting of those vectors (polynomials) x for which

(a) x has degree 4,

(b) $2x(0) = x(1)$,

(c) $x(t) \geq 0$ whenever $0 \leq t \leq 1$,

(d) $x(t) = x(1 - t)$ for all t.

In which of these cases is $\mathcal{V}$ a vector space?

Solution Just like in the previous excercise, $\mathcal{V}$ has the same linear operations of addition and scalar multiplication as the vector space $\mathcal{P}$ over $\mathbb{R}$. Hence, for the subset $\mathcal{V}_x$ of case x, it suffices to check if $0 \in \mathcal{V}_x$, each vector has its unique inverse and $\mathcal{V}_x$ is closed under this linear operations to conclude that it is a vector space. Here, 0 is the polynomial $p(t) = 0$ for all $t \in \mathbb{R}$. Then, (a) and (c) are not vector spaces because

$$0 \notin \mathcal{V}_a \text{ (no additive identity) since 0 has no degree 4 and}$$
$$\text{if } x(t) \in \mathcal{V}_c \text{ and } x(1) > 0, \text{ then } -x(t) \notin \mathcal{V}_c \text{ (no additive inverse)}$$

since $-x(1) = (-1) \cdot x(1) < 0$. On the other hand, $0 \in \mathcal{V}_b, \mathcal{V}_d$ since $2 \cdot p(0) = p(1) = 0$ and $p(t) = p(1-t) = 0$ for all $t \in \mathbb{R}$. Furthermore, if $x(t) \in \mathcal{V}_b$, then $2 \cdot (-x(0)) = (2(-1)) \cdot x(0) = -1 \cdot (2 \cdot x(0)) = (-1) \cdot x(1) = -x(1)$ and so $-x(t) \in \mathcal{V}_b$. Also, for some $x_1, x_2 \in \mathcal{V}_b$ and $\alpha \in \mathbb{R}$,

$$\begin{aligned} 2 \cdot (x_1 + x_2)(0) &= 2 \cdot (x_1(0) + x_2(0)) = x_1(1) + x_2(1) \\ &= (x_1 + x_2)(1) \end{aligned}$$

and

$$\begin{aligned} 2 \cdot (\alpha \cdot x_1(0)) &= (\alpha 2) \cdot x_1(0) = \alpha \cdot (2 \cdot x_1(0)) \\ &= \alpha \cdot x(1). \end{aligned}$$

Now consider some $x_1, x_2 \in \mathcal{V}_d$ and $\alpha \in \mathbb{R}$. Then, $-x(t) = (-1) \cdot x(t) = (-1) \cdot x(1-t) = -x(1-t)$ for every $t \in \mathbb{R}$. Moreover,

$$\begin{aligned} (x_1 + x_2)(t) &= x_1(t) + x_2(t) = x_1(1-t) + x_2(1-t) \\ &= (x_1 + x_2)(1-t) \end{aligned}$$

and

$$\alpha \cdot x_1(t) = \alpha \cdot x_1(1-t)$$

for any $t \in \mathbb{R}$. Hence, $\mathcal{V}_b$ and $\mathcal{V}_d$ are vector spaces.

3 Properties of sets of vectors: Linear dependence and Linear combinations

3.1 Linear dependence

Now that we have described these sets with specific characteristics known as **Vector Spaces** over some field, we can explore some interesting properties that their subsets can have. But first, let's define the summation notation $\sum_i x_i$ for vectors of a vector space $\mathcal{V}$. The set $\{x_i\}$ is a subset of $\mathcal{V}$ where $i \in I$ are the indexes. Then,

$$\sum_i x_i = x_{i_1} + x_{i_2} + \ldots x_{i_n}$$

namely, the sequent application of addition for the vectors $\{x_i\}$. Furthermore, if $I = \emptyset$, then $\{x_i\} = \emptyset$ and $\sum_i x_i$ is defined to be the vector 0 since there are no indexes to assign to vectors.

Now, we can proceed with the discussion of linear dependence. A finite subset $\{x_i\} \subseteq \mathcal{V}$ is linearly dependent if there exists a set $\{\alpha_i : \exists i, \alpha_i \neq 0\}$ of scalars such that $\sum_i \alpha_i x_i = 0$. On the other hand, by negation, it is linearly independent if no such set exists. This can be interpreted as that for every set $\{\alpha_i : \exists i, \alpha_i \neq 0\}$ of scalars, $\sum_i \alpha_i x_i \neq 0$. Because we are dealing with scalars of a field and $0x = 0$, it is true that, in the case of a linearly independent set $\{x_i\}$,

$$\sum_i \alpha_i x_i = 0 \iff \forall i \in I, \alpha_i = 0.$$

One can push the limits of this ideas and ask in which category does the empty set $\emptyset \subseteq \mathcal{V}$ resides. After all, it is a finite subset of $\mathcal{V}$. The issue with this, is that $\{x_i\} = \emptyset$ implies that $\{i\} = \emptyset$, namely, we don't have indexes to assign to something since there are not things to be assigned (vectors). However, note that

$$\{i\} = \emptyset \implies \sim \left(\exists \left\{ \alpha_i : \exists i, \alpha_i \neq 0 \right\}, \sum_i \alpha_i x_i = 0 \right)$$

since we don't have indexes to assign to scalars and so there is no i such that $\alpha_i \neq 0$. This implies that no such set $\{\alpha_i : \exists i, \alpha \neq 0\}$ can be constructed. Hence, by definition, the empty set is linearly independent. Obviously, this argument uses the excluded middle principle, and is open for debate.
In the case of not finite set $\mathcal{M}$ of vectors, we say that $\mathcal{M}$ is linearly dependent if every finite subset is linearly dependent.

Recall that every field over itself is a vector space. Let $\mathcal{V}$ be an example of such vector space. Then, consider the set $S = \{x, y\} \subseteq \mathcal{V}$. If $x = y = 0$, then S is linearly dependent. If not, $(-x)y + (y)x = 0$. Hence, every subset of $\mathcal{V}$ containing two vectors is linearly dependent. Using mathematical induction, one can conclude that any finite subset such that $|S| \geq 2$ is linearly dependent. However, $\mathcal{V}$ is not linearly dependent, since $\{x\}$ for any nonzero $x \in \mathcal{V}$ is linearly independent. This has to do with the uniqueness of 0 as the additive identitiy.

Furthermore, a vector x is a linear combination of the set $\{x_i\}$ if $x = \sum_i \alpha_i x_i$. Note that, by definition, 0 is linearly dependent on the emptyset. It is common to say that x is linearly dependent on $\{x_i\}$. This is so due to the following thorem.

Theorem 1. Let x be a vector in the vector space $\mathcal{V}$ and $\{x_i\} \subseteq \mathcal{V}$ be linearly independent. Then, the set $\{x\} \cup \{x_i x\}$ is linearly dependent if and only if $x = \sum_i \alpha_i x_i$.

Proof. Assume that $\{x_i\} \cup \{x\}$ is linearly dependent. Hence, there is a set $S_j = \{\alpha_j : \exists j, \alpha_j \neq 0\}$ such that $\sum_j \alpha_j x_j = 0$, here j is the new index notation for $\{x_i\} \cup \{x\}$. Since $\{x_i\}$ is linearly independent, it follows that the coefficient α of x can not be 0 since there is no set S_i such

that $0x + \sum_i \alpha_i x_i = 0$. Hence,

$$x = \alpha^{-1}\left(\sum_i -\alpha_i x_i\right),$$

and so x is a linear combination of $\{x_i\}$. Note that the scope of the argument includes the case when $\{x_i\} = \emptyset$. For the converse, assume that $x = \sum_i \alpha_i x_i$ and so $(1)x - \sum_i \alpha_i x_i = 0$. Therefore, $1 \in \{\alpha_j\} \supseteq \{\alpha_i\}$ and the set $\{x_j\} = \{x_i\} \cup \{x\}$ is linearly dependent. □

Additionaly, a set of non-zero vectors $\{x_n\}$ is linearly dependent if and only if some x_k, $2 \leq k \leq n$, is a linear combination of the preceding ones. Another concept that was explained is basis. Basically, a basis is a linearly independent subset of some vector space such that any vector is a linear combination of it. Interestingly, for any finite vector space, one can extend any linearly independent subset to a basis by adding vectors to it. In the case of the vector space $\{0\}$, its basis is the empty set. Also, a vector space with a finite basis is known as a **finite-dimensional vector space**.

Problem 1. (a) Prove that th four vectors

$$\begin{aligned} x &= (1,0,0) \\ y &= (0,1,0) \\ z &= (0,0,1) \\ u &= (1,1,1), \end{aligned}$$

in $\mathcal{C}^2$ form a linearly dependent set, but any three of them are linearly independent.

Proof. Let $S = \{x, y, z, u\}$. Note that $u = x+y+z = (1,1,1)$ and so $u-(x+y+z) = 0$ and so the set of scalars $\{\alpha_i\}$ contains nonzero elements. Hence, S is linearly dependent. Now, consider some subset $P \subseteq S$ with only three elements. Since three of the four vectors have only one nonzero element in one unique place of the ordered triple, it follows that P contains at least two of this vectors. Then, this two vectors coincide in having a zero element in the i'th place of the ordered triple, and the third vector has a nonzero element in place i. Hence, $0 \cdot \gamma_i = 0$, being γ_i the i'th element of the third vector, implies that $\alpha_3 = 0$. Furthermore, the first two mentioned vectors do not coincide in their nonzero elements and so $\alpha_1 x + \alpha_2 y = 0 \implies \alpha_1, \alpha_2 = 0$. Therefore, P is linearly independent. □

(b) If the vectors x, y, z, and u in $\mathcal{P}$ are defined by $x(t) = 1$, $y(t) = t$, $z(t) = t^2$, and $u(t) = 1 + t + t^2$, prove that x, y, z, and u are linearly dpenden, but any three of them are linearly dependent.

Proof. Let $S = \{x, y, z, u\}$. Observe that $u(t) = 1+t+t^2 = (1)x(t)+(1)y(t)+(1)z(t)$. Hence, u, a nonzero vector, is a linear combination of x, y, z and so S is a linearly

dependent set. Note that

$$\begin{aligned} x(t) = 1 + 0t + 0t^2 &\mapsto (1, 0, 0) \\ y(t) = 0 + t + 0t^2 &\mapsto (0, 1, 0) \\ z(t) = 0 + 0t + t^2 &\mapsto (0, 0, 1) \\ u(t) = 1 + t + t^2 &\mapsto (1, 1, 1), \end{aligned}$$

which is the same set of vectors that we saw earlier. Hence, by the same argument, any subset $P \subset S$ of three vectors is linearly independent. □

Problem 2. Prove that if $\mathbb{R}$ is considered as a rational vector space (a vector space over $\mathbb{Q}$), then a necessary and sufficient condition that the vectors 1 and ξ in $\mathbb{R}$ be linearly independent is that the real number ξ be irrational.

Proof. Suppose that ξ is irrational. Then, $\alpha \cdot 1 + \beta \cdot \xi$, where $\alpha, \beta \in \mathbb{Q}$ and $\beta \neq 0$, is an irrational number and thus nonzero. If $\beta = 0$, then $\alpha \cdot 1$ is zero if and only if $\alpha = 0$. Therefore, $\{1, \xi\}$ is a linearly independent set.
For the converse, assume that $\{1, \xi\}$ is linearly independent. We know that ξ being irrational and $\{1, \xi\}$ is linearly independent are both true. Then, we only have to show that this is not the case when ξ is rational. Suppose that ξ is rational. If $\xi = 0$, then $0 \cdot 1 + 3 \cdot 0 = 0$. On the other hand, $\xi \cdot 1 + (-1) \cdot \xi = 0$ for any nonzero ξ. □

Problem 3. Is it true that if x, y, and z are linearly independent vectors, then so also are $x + y$, $y + z$, and $z + x$?

Proof. Yes, the set $A = \{x + y, y + z, z + x\}$ is linearly independent. First, consider any field $\mathcal{B}$. Let $\{\alpha, \beta, \gamma\} \subseteq \mathcal{B}$, where at least one of them is nonzero. Then,

$$\alpha(x + y) + \beta(y + z) + \gamma(z + x) = (\alpha + \gamma)x + (\alpha + \beta)y + (\beta + \gamma)z.$$

Since one of the scalars is nonzero, it follows that two scalars must be the inverse additive of this nonzero scalar for two of the sums to be zero, which implies that their sum is nonzero. Hence, at least one of the sums $\alpha + \beta, \alpha + \gamma, \gamma + \beta$ is nonzero. Thus, $(\alpha + \gamma)x + (\alpha + \beta)y + (\beta + \gamma)z \neq 0$ (recall that $\{x, y, z\}$ is linearly independent). □

Problem 4. (a) Under what conditions on the scalar ξ are the vectors $(1 + \xi, 1 - \xi)$ and $(1 - \xi, 1 + \xi)$ in $\mathbb{C}^2$ linearly dependent?

Proof. The vectors are linearly dependent if and only if $\xi = 0$. Clearly, the vectors are equal when $\xi = 0$ and so linearly dependent. For the converse, assume that the vectors are linearly dependent. Hence, there are scalars α and β such that $\alpha(1 + \xi, 1 - \xi) + \beta(1 - \xi, 1 + \xi) = 0$, where at least one of them, say α, is nonzero. Then,

$$(\alpha + \beta + (\alpha - \beta)\xi, \alpha + \beta - (\alpha - \beta)\xi) = 0.$$

Hence, $\alpha + \beta = -(\alpha - \beta)\xi$ and so $2(\alpha + \beta) = 0$. This further implies that $\alpha = -\beta \neq 0$. Thus, $-(-2\beta)\xi = 0$ and so $\xi = 0$. □

(b) Under what conditions on the scalar ξ are the vectors $(\xi, 1, 0), (1, \xi, 1)$ and $(0, 1, \xi)$ in $\mathbb{R}^3$ linearly dependent?

Proof. Let these vectors be linearly dependent. Then, there are some scalars $\alpha, \beta, \gamma \in \mathbb{R}$ such that

$$\alpha(\xi, 1, 0) + \beta(1, \xi, 1) + \gamma(0, 1, \xi) = 0,$$

where at least one of them is nonzero. Then,

$$\alpha\xi = \gamma\xi = -\beta \qquad \text{and} \qquad \alpha + \gamma + \beta\xi = 0.$$

If $\xi = 0$, then $\beta = 0$ and $\alpha = -\gamma \neq 0$. Now, let's consider the case when $\xi \neq 0$. Then, the left equation implies that $\gamma = \alpha = -\beta/\xi$ and so $\beta \neq 0$ (at least one of the scalars is nonzero). Futhermore,

$$\begin{aligned} \alpha + \gamma + \beta\xi &= 2\gamma + \beta\xi \\ &= -2\beta/\xi + \beta\xi = 0. \end{aligned}$$

With algebraic manipulations, one can conclude that $|\xi| = \sqrt{2}$. □

(c) What is the answer to (b) for $\mathbb{Q}^3$ (in place of $\mathbb{R}^3$)?

Proof. From (b), it is evident that the vectors are linearly dependent if and only if $\xi = 0, \pm\sqrt{2}$. Hence, the vectors are linearly dependent in $\mathbb{Q}^3$ if and only if $\xi = 0$ since $\mathbb{Q}^3 \subset \mathbb{R}^3$. □

Problem 5. (a) The vectors (ξ_1, ξ_2) and (η_1, η_2) in $\mathbb{C}^2$ are linearly dependent if and only if $\xi_1\eta_2 = \xi_2\eta_1$.

Proof. Assume that $\eta_2\xi_1 = \xi_2\eta_1$. Then,

$$\begin{aligned} \eta_1(\xi_1, \xi_2) - \xi_1(\eta_1, \eta_2) &= (\eta_1\xi_1 - \xi_1\eta_1, \eta_1\xi_2 - \xi_1\eta_2) \\ &= 0. \end{aligned}$$

For the converse, suppose that the vectors are linearly dependent. Then, one can be expressed as the other multiplied by a constant (since they are linearly dependent, the two scalars must be nonzero so that the sum of the vectors multiplied by their respective scalar is zero). Hence, $(\eta_1, \eta_2) = c(\xi_1, \xi_2)$. Thus, $\eta_1 = c\xi_1$ and $\eta_2 = c\xi_2$. Multiplying the left equality by η_2, we get $c\xi_2\eta_1 = c\xi_1\eta_2$. Because $c \neq 0$, $\eta_1\xi_2 = \xi_1\eta_2$. □

(b) Find a similar necessary and sufficient condition for the linear dependence of two vectors in $\mathbb{C}^3$. Do the same for three vectors in $\mathbb{C}^3$.

Solution Two vectors (ξ_1, ξ_2, ξ_3) and (η_1, η_2, η_3) are linearly dependent if and only if $\xi_i\eta_j = \eta_i\xi_j$ for any $i, j \in \{1, 2, 3\}$.

Proof. Assume that $\xi_i\eta_j = \eta_i\xi_j$ for any $i, j \in \{1, 2, 3\}$. Then, for some $i \in \{1, 2, 3\}$,

$$\begin{aligned}\eta_i(\xi_1, \xi_2, \xi_3) - \xi_i(\eta_1, \eta_2, \eta_3) &= (\eta_i\xi_1 - \xi_i\eta_1, \eta_i\xi_2 - \xi_i\eta_2, \eta_i\xi_3 - \xi_i\eta_3) \\ &= 0.\end{aligned}$$

For the converse, suppose that these vectors are linearly dependent. Then, $\xi_1 = c\eta_1, \xi_2 = c\eta_2$ and $\xi_3 = c\eta_3$. Generally, we have $\xi_i = c\eta_i$ for any $i \in \{1, 2, 3\}$. Then, for some $j \in \{1, 2, 3\}$, $c\eta_j\xi_i = c\eta_i\xi_j$. Since $c \neq 0$, it follows that $\eta_j\xi_i = \eta_i\xi_j$ for any $i, j \in \{1, 2, 3\}$. □

For any 3 vectors $(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3) \in \mathcal{C}^3$, they are linearly dependent if and only if

$$a_1b_3c_2 + a_3b_2c_1 + a_2b_1c_3 = a_2b_3c_1 + a_1b_2c_3 + a_3b_1c_2.$$

(Note the ones on the left have indexes ordered in an improper permutation, the opposite is seen on the right-side).

Proof. First, assume the latter for some set of linearly independent vectors in $\mathbb{C}^3$. Then, consider the following linear combination,

$$\begin{aligned}([b_2c_3 - b_3c_2] + [a_3c_2 - a_2c_3] + [a_2b_3 - a_3b_2]) \cdot (a_1, b_1, c_1) + \\ ([b_3c_1 - b_1c_3] + [a_1c_3 - a_3c_1] + [a_3b_1 - a_1b_3]) \cdot (a_2, b_2, c_2) + \\ ([b_1c_2 - b_2c_1] + [a_2c_1 - a_1c_2] + [a_1b_2 - a_2b_1]) \cdot (a_3, b_3, c_3)\end{aligned}$$

For the converse, suppose that these vectors are linearly dependent. Then, there are scalars $a, b, c \in \mathbb{C}$ such that $ax_1 + bx_2 + cx_3 = 0$ and at least one of them, say α, is nonzero. Hence,

$$\begin{aligned}a_1 &= \beta a_2 + \gamma a_3 \\ b_1 &= \beta b_2 + \gamma b_3 \\ c_1 &= \beta c_2 + \gamma c_3.\end{aligned}$$

If only the scalar a is nonzero, then $x_1 = 0$ (the vectors are linearly dependent) and so $0b_3c_2 + 0b_2c_1 + 0b_1c_3 = 0 = 0b_3c_1 + 0b_2c_3 + 0b_1c_2$. If only two are nonzero, say a and b, then, by the previous result for a linearly dependent set of two vectors, $a_1(b_3c_2 - b_2c_3) + a_3(b_2c_1 - b_1c_2) + a_2(b_1c_3 - b_3c_1) = (a_1 + a_2 + a_3)0 = 0$. Thus, we can assume that all scalars are nonzero and so $\beta, \gamma \neq 0$.
Now, note that $a_1(\beta b_2 + \gamma b_3) = b_1(\beta a_2 + \gamma a_3)$ and so

$$\gamma c_3(\beta a_1b_2 - \beta a_2b_1) = c_1(\gamma a_3b_1 - \gamma a_1b_3) - \beta c_2(\gamma a_3b_1 - \gamma a_1b_3) \tag{1}$$

$$\gamma\beta(a_1b_2c_3 - a_2b_1c_3) = -\gamma\beta(a_3b_1c_2 - a_1b_3c_2) + \gamma a_3b_1c_1 - \gamma a_1b_3c_1. \tag{2}$$

Let's find some useful equalities for $\gamma a_1b_3c_1$ and $\gamma a_3b_1c_1$ for substitution in the previous equality. Note that

$$\begin{aligned}\gamma\beta(a_1c_2b_3 - a_2c_1b_3) &= -\gamma\beta(a_3c_1b_2 - a_1c_3b_2) + \gamma a_3c_1b_1 - \gamma a_1c_3b_1 \\ \gamma\beta(c_1b_2a_3 - c_2b_1a_3) &= -\gamma\beta(c_3b_1a_2 - c_1b_3a_2) + \gamma c_3b_1a_1 - \gamma c_1b_3a_1\end{aligned}$$

by interchanging b and c, and a and c in equation (2), respectively. It's like using the same algorithm to derive (2) but interchanging the position of letters (placeholders). Hence,

$$\gamma\beta(a_1b_2c_3 - a_2b_1c_3 + a_3b_1c_2 - a_1b_3c_2) = \gamma\beta(a_1c_2b_3 - a_2c_1b_3 + a_3c_1b_2 - a_1c_3b_2) + \gamma a_1c_3b_1$$
$$+\gamma\beta(c_1b_2a_3 - c_2b_1a_3 + c_3b_1a_2 - c_1b_3a_2) - \gamma c_3b_1a_1 \implies$$
$$2\gamma\beta(a_1b_2c_3 + a_3b_1c_2 + a_2b_3c_1) = 2\gamma\beta(a_2b_1c_3 + a_1b_3c_2 + a_3b_2c_1).$$

Therefore,

$$a_1b_3c_2 + a_3b_2c_1 + a_2b_1c_3 = a_2b_3c_1 + a_1b_2c_3 + a_3b_1c_2.$$

□

(c) Is there a set of three linearly independent vectors $\mathbb{C}^2$?

Problem 8. (a) Under what conditions on the scalar ξ do the vectors $(1, 1, 1)$ and $(1, \xi, \xi^2)$ form a basis of $\mathbb{C}$?

Solution We know that for any $n \in \mathbb{N}$, the basis of $\mathbb{C}^n$ must contain at least n vectors. Furthermore, these must be linearly independent. Otherwise,

$$x_1 = \alpha_2x_2 + \alpha_3x_3 + \cdots + \alpha_nx_n$$

for some x_1 and scalars $\alpha_2, \ldots, \alpha_n$, and so the linear combination $\sum_{i=1}^n \beta_ix_i = \sum_{i=2}^n(\alpha_i\beta_1 + \beta_i)x_i$ is a linear combination of $n - 1$ vectors.

Then, since there are two vectors and the vector space is $\mathbb{C}$, it follows that we just have to look for a condition for them to be lineraly independent. Then, this vectors form a basis if and only if $\xi \neq 1$.

Proof. Assume that the vectors are linearly dependent. Then, $(1, \xi, \xi^2) = c(1, 1, 1)$ for some nonzero $c \in \mathbb{C}$. Then, $1 = \xi = \xi^2$ and so $\xi = 1$.

For the converse, suppose that $\xi \neq 1$. Then, $\xi < \xi^2$ and so there is no nonzero scalar c such that $(1, \xi, \xi^2) = c(1, 1, 1)$. □

(b) Under what conditions on the scalar ξ do the vectors $(0, 1, \xi), (\xi, 0, 1)$, and $(\xi, 1, 1 + \xi)$ form a basis of $\mathbb{C}^3$.

Solution Note that for any $\xi \in \mathbb{C}$,

$$(0, 1, \xi) = -(\xi, 0, 1) + (\xi, 1, 1 + \xi).$$

Hence, for every $\xi \in \mathbb{C}$, the vectors are linearly dependent and so not a basis of $\mathbb{C}^3$. There are no conditions for them to be a basis.

Problem 10. If $\mathcal{X}$ is the set consisting of the six vectors $(1,1,0,0),(1,0,1,0),(1,0,0,1),(0,1,1,0)$, $(0,1,0,1),(0,0,1,1)$ in $\mathcal{C}^4$, find two different maximal linearly independent subsets of $\mathcal{X}$. (A maximal linearly independent subset of $\mathcal{X}$ is a linearly independent subset $\mathcal{Y}$ of $\mathcal{X}$ that becomes linearly dependent every time that a vector $\mathcal{X}$ that is not already in $\mathcal{Y}$ is adjoined to $\mathcal{Y}$).

Solution Two maximal linearly independent subsets are $(0,0,1,1),(0,1,0,1)$, $(0,1,1,0),(1,0,0,1),(1,1,0,0)$ and $(1,1,0,0),(1,0,1,0),(1,0,0,1),(0,1,1,0)$. Note that we can divide the vectors in two groups, the ones with number 1 as the first entry and the ones with a 0. Furthermore, the last three entries of the vectors of each group are linearly independent and so they span the last three entries of each vector from the other group.

4 Classification of Finite Vector Spaces: dimension and isomorphism

We know that a basis of some Vector Space $\mathcal{V}$ is a subset that is both linearly independent and a generator of $\mathcal{V}$. One can show, by repeatedly using the fact that a set is linearly independent if and only if the preceding vectors span it, that a linearly independent set has less or equal number of vectors than a generator set. Hence, any basis of the same vector space has the same number of elements.
This is a very useful fact, which the concept of *Dimension* harnesses. One can categorize Vector Spaces into sets according to their dimension, namely, the number of elements that its basis has. Furthermore, for any n finite dimensional vector space $\mathcal{U}$ over $\mathbb{F}$ with basis $(x_\alpha)_{\alpha\in\mathbb{N}}$, there is the isomorphism $\phi:\mathcal{U}\to\mathbb{F}^n$ such that

$$x\to(\lambda^\alpha)_{\alpha\in\mathbb{N}}, x=\sum\lambda_\alpha x_\alpha.$$

since there is a one-to-one correspondence between the vector x and scalars λ_α. With this, one concludes this connects vector spaces in a way such that there is an isomorphism between two vector spaces if and only if the have the same dimension.

Problem 1. (a) What is the dimension of the set $\mathbb{C}$ of all complex numbers considered as a real vector space?

Solution So the field is $\mathbb{R}$ and there is a one-to-one correspondence between each number $a+bi\in\mathbb{C}$ and $(a,b)\in\mathbb{R}^2$, which is also a real vector space. Hence the dimension of the real vector space $\mathbb{C}$ is 2. From this, we can prove the following useful theorem:

Theorem Isomorphism-dimension:. There is an isomorphism between two finite vector spaces over the same field if and only if they have the same dimension.

Proof. Let $\mathcal{V}$,$\mathcal{U}$ be vector spaces over the same field such that $\mathcal{V}\leftrightarrows\mathcal{U}$, there is an isomorphism T. Both have unique basis, and so let $(x_\lambda)_{\lambda\leq n}$ be the basis of $\mathcal{V}$. We show

that $(T(x_\lambda))_{\lambda\leq n}$ is the basis of $\mathcal{U}$. Consider any vector $u \in \mathcal{U}$. By the surjectivity of T, there is some $v \in \mathcal{V}$ such that $T(v) = u$ and so,

$$T(\sum_{\lambda\leq n} \alpha_\lambda x_\lambda) = \sum_{\lambda\leq n} \alpha_\lambda T(x_\lambda).$$

Furthermore, if $u = 0$, then $\alpha_\lambda = 0$ and so $(T(x_\lambda))$ is linearly independent and a generator of $\mathcal{U}$. It is the basis of $\mathcal{U}$.
To prove the converse, it suffices to note that $\mathcal{V} \leftrightarrows \mathbb{F}^n \leftrightarrows \mathcal{U}$, where $\mathbb{F}$ is the field of both vector spaces. □

Every complex vector space $\mathcal{V}$ is intimately associated with a real vector space $\mathcal{V}^-$; the space $\mathcal{V}^-$ is obtained from $\mathcal{V}$ by refusing to multiply vectors of $\mathcal{V}$ by anything other than real scalars. If the dimension of the complex vector space $\mathcal{V}$ is n, what is the dimension of the real vector space $\mathcal{V}^-$.

Proof. The dimension of $\mathcal{V}^-$ is $2n$. We use the notation $\mathbb{R}|\mathcal{C}$ to represent the vector space $\mathcal{C}$ over $\mathbb{R}$. Note that

$$\begin{aligned}\mathbb{C}|\mathcal{V} &\leftrightarrows \mathbb{C}|\{(a_1 + b_1 i, \ldots, a_n + b_n i) : a_1, b_1, \ldots, a_n, b_n \in \mathbb{R}\}\\ &\leftrightarrows \mathbb{C}|\{(a_1, b_1, \ldots, a_n, b_n)|a_1, \ldots, b_n \in \mathbb{R}\} = \mathbb{C}|\mathbb{R}^{2n}.\end{aligned}$$

Hence, $\mathbb{R}|\mathcal{V} \leftrightarrows \mathbb{R}|\mathbb{R}^{2n}$ and so the dimension of $\mathcal{V}^-$ is $2n$. □

Problem 2. Is the set $\mathbb{R}$ of all real numbers a finite-dimensional vector space over the field $\mathbb{Q}$ of all rational numbers? (The question is not trivial; it helps to know something about cardinal numbers.)

Solution An argument by contradiction can be given. Suppose, to the contrary, that this was true, then, clearly, $\mathbb{Q}|\mathbb{R} \leftrightarrows \mathbb{Q}|\mathbb{Q}^n$ for some n. However,

$$\begin{aligned}\mathbb{N} \sim \mathbb{Q}|\mathbb{Q}^n &\leftrightarrows \mathbb{Q}|\mathbb{R}\\ &\supseteq \{1b|b \in \mathbb{R}\} = \mathbb{R}.\end{aligned}$$

Because the multiplication is closed in the set of real numbers, $\mathbb{Q}|\mathbb{R} = \mathbb{R}$. This implies that $\mathbb{R}$ is countable, which is not true. We arrive at a contradiction.
A corollary from this is that a finite vector space over a countable field is countable.

Proof. Let $\mathbb{D}|\mathcal{V}$ be a finite dimensional set (finite basis with n elements) over some countable field $\mathbb{D}$. Then, $\mathbb{D}|\mathbb{D}^n = \mathbb{D}^n \sim \mathbb{N}^n \sim \mathbb{N}$. Thus, the biyection (isomorphism) between $\mathbb{D}|\mathcal{V}$ and $\mathbb{D}^n$ implies that the earlier is countable. □

Problem 3. How many vectors are there in an n-dimensional vector space over the field $\mathbb{Z}_p$ (where p is a prime)?

Solution Let $\mathcal{V}$ be such vector space. Then, $\mathcal{V} \leftrightarrows \mathbb{Z}_p|\mathbb{Z}_p^n \leftrightarrows \mathbb{Z}_p^n$. Therefore, $|\mathbb{Z}_p^n| = p^n = |\mathcal{V}|$.

Problem 4. Discuss the following assertion: if two rational vector spaces have the same cardinal number (i.e., if there is some one-to-one correspondence between them), they are isomorphic (i.e., there is a linearit-preserving one-to-one correspondence between them). A knowledge of the basic facts of cardinal arithmetic is needed for an intelligent discussion.

Solution

4.1 Subspaces: A new perspective into basis and the concept of "span"

Before diving into the interesting idea and usage of subsapces, we must account of some fundamental facts of vector spaces. First of all, we defined a basis $\mathcal{M}$ as a linearly independent subset of a vector space $\mathcal{V}$ such that every vector in $\mathcal{V}$ can be expressed as a linear combination of the vectors in $\mathcal{M}$. Then, using Zorn's Lemma and the fact that a set is linearly dependent if at least one vector is a linear combination of the previous ones, one can show that every vector space has at least one basis and that the cardinality is the same for all possible basis, respectively.

Now, a subspace $\mathcal{M}$ of a $\mathbb{F}|\mathcal{V}$ is a subset such that if $x, y \in \mathcal{M}$, then $\alpha x + \beta y \in \mathcal{M}, \alpha, \beta \in \mathbb{F}$. Clearly, this is a vector space when restricted to the operations of addition and scalar multiplication from $\mathcal{V}$ (Note that $x - x \in \mathcal{M}$). Furthermore, for any collection $\{\mathcal{M}_p\}$ of subsapces, their intersection $\bigcap_p \{\mathcal{M}_p\} \supseteq \mathcal{O} = \{0\}$ is a vector space.

This is useful, because for any linearly independent set of vectors $\mathcal{S} \subset \mathcal{V}$, we can find the intersection of all subspaces that cointain S, whic can be shown to be equivalent to the set of all linear combinations of the vectors in $\mathcal{S}$. Sounds familiar?. Indeed, this $\mathcal{S}$ is a basis for $\mathcal{M}$. Hence, a new way to look at a basis is the linearly independent set of vectors such that $\mathcal{M}$ is the set of all linear combinations of these vectors. Then, it is said that the linearly independent set "spans" $\mathcal{M}$. Also, the dimension of $\mathcal{M}$ is the cardinality of this linearly independent set.

Problem 1. If $\mathcal{M}$ and $\mathcal{N}$ are finite-dimensional subspaces with the same dimension, and if $\mathcal{M} \subset \mathcal{N}$, then $\mathcal{M} = \mathcal{N}$.

Proof. Since $\mathcal{M} \subset \mathcal{N}$, it follows that $\mathcal{M}$ is a subspace of the vector space $\mathcal{N}$. Hence, by theorem 2, we can find a basis K in $\mathcal{N}$ so that $L \subseteq K$ forms a basis in $\mathcal{M}$. However, both vector spaces have the same dimension and so $|K| = |L| = n$, which implies that $K = L$. Thus, $\mathcal{M} = \mathcal{N}$. □

Problem 2. If $\mathfrak{M}$ and $\mathfrak{N}$ are subspaces of a vector space $\mathfrak{V}$, and if every vector in $\mathfrak{V}$ belongs either to $\mathfrak{M}$ or to $\mathfrak{N}$ (or both), then either $\mathfrak{M} = \mathfrak{V}$ or $\mathfrak{N} = \mathfrak{V}$ (or both).

Proof. Suppose, without loss of generality, that every vector in $\mathfrak{V}$ belongs to $\mathfrak{M}$. Then, $\mathfrak{V} \subseteq \mathfrak{M}$ and $\mathfrak{M} \subseteq \mathfrak{V}$, since $\mathfrak{M}$ is a subspace of $\mathfrak{V}$. Hence, $\mathfrak{M} = \mathfrak{V}$. □

Problem 3. If x, y, and z are vectors such that $x + y + z = 0$, then x and y span the same subspace as y and z.

Proof. Consider the subspaces $\mathfrak{Z} = \{\gamma z : \gamma \in \mathbb{F}\}, \mathfrak{X} = \{\alpha x : \alpha \in \mathbb{F}\}$ and $\mathfrak{Y} = \{\beta y : \beta \in \mathbb{F}\}$, where $\mathbb{F}$ is the field. Then,

$$\begin{aligned}
\mathfrak{X} + \mathfrak{Y} &= \{\alpha x + \beta y : \alpha, \beta \in \mathbb{F}\} \\
&= \{\alpha(z - y) + \beta y : \alpha, \beta \in \mathbb{F}\} \\
&= \{\alpha z + \gamma y : \alpha, \gamma \in \mathbb{F}\} \\
&= \mathfrak{Y} + \mathfrak{Z}
\end{aligned}$$

because $\mathbb{F}$ is closed under addition. $\square$

From this, we can easily derive a corollary:

If $x_1 + x_2 + \cdots + x_n = 0$, then any subspace spanned by a pair of the vectors x_k spans the space spanned by the rest plus at least one of the pair. The need of a pair must have to do with the binary nature of addition.

Problem 4. Suppose that x and y are vectors and $\mathfrak{M}$ is a subspace in a vector space $\mathfrak{V}$; let $\mathfrak{H}$ be the subspace spanned by $\mathfrak{M}$ and x, and let $\mathfrak{K}$ be the subspace spanned by $\mathfrak{M}$ and y. Prove that if y is in $\mathfrak{H}$ but not in $\mathfrak{M}$, then x is in $\mathfrak{K}$.

Proof. We know that $\{\alpha x\} + \mathfrak{M} = \mathfrak{H}$ and $\{\beta y\} + \mathfrak{M} = \mathfrak{K}$. Since $y \in \mathfrak{H}$, it follows that $y = \alpha x + m$ for some $m \in \mathfrak{M}$. Furtheremore, $\alpha \neq 0$ because $y \notin \mathfrak{M}$. Thus, $x = \alpha^{-1}y - \alpha^{-1}m \in \mathfrak{K}$. $\square$

Problem 5. Suppose that $\mathfrak{L}, \mathfrak{M}$, and $\mathfrak{N}$ are subspaces of a vector space.

(a) Show that the equation

$$\mathfrak{L} \cap (\mathfrak{M} + \mathfrak{N}) = (\mathfrak{L} \cap \mathfrak{M}) + (\mathfrak{L} \cap \mathfrak{N})$$

is not necessarily true.

Proof. Let $\mathfrak{M} = \{\alpha m\}, \mathfrak{N} = \{\alpha n\}$ and $\mathfrak{L} = \{\alpha(n+m)\}$, where $\{m, n\}$ are linearly independent. Then,

$$\begin{aligned} \mathfrak{L} \cap (\mathfrak{M} + \mathfrak{N}) &= \mathfrak{L} \\ &\neq \{0\} = \mathfrak{L} \cap \mathfrak{M} + \mathfrak{L} \cap \mathfrak{N}. \end{aligned}$$

The subspaces $\mathfrak{L}, \mathfrak{M}, \mathfrak{N}$ can be seen as lines in the plane $\mathfrak{M} + \mathfrak{N}$ that only intersect at the origin. $\square$

(b) Prove that

$$\mathfrak{L} \cap (\mathfrak{M} + (\mathfrak{L} \cap \mathfrak{N})) = (\mathfrak{L} \cap \mathfrak{M}) + (\mathfrak{L} \cap \mathfrak{N})$$

Proof. Let $\mathfrak{B} = \mathfrak{L} \cap \mathfrak{N}$. Since $0 \in \mathfrak{M}, \mathfrak{B}$, it follows that $\{m + 0\} = \mathfrak{M}$ and $\{b + 0\} = \mathfrak{B}$ are subsets of $\mathfrak{M} + \mathfrak{B}$ and so

$$\begin{aligned} \mathfrak{B}, \mathfrak{L} \cap \mathfrak{M} \subseteq \mathfrak{L} \cap (\mathfrak{M} + \mathfrak{B}) \implies \\ \mathfrak{L} \cap \mathfrak{M} + \mathfrak{B} \subseteq \mathfrak{L} \cap (\mathfrak{M} + \mathfrak{B}). \end{aligned}$$

Now, consider any $x \in \mathfrak{L} \cap (\mathfrak{M} + (\mathfrak{L} \cap \mathfrak{N}))$. Then, $x = m + n$, where $m \in \mathfrak{M}$ and $n \in \mathfrak{N} \cap \mathfrak{L}$. Then, $-n \in \mathfrak{L} \cap (\mathfrak{M} + \mathfrak{N} \cap \mathfrak{L})$ and so $m + n - n = m \in \mathfrak{L} \cap (\mathfrak{M} + \mathfrak{N} \cap \mathfrak{L})$. Thus, $m \in \mathfrak{L} \cap \mathfrak{M}$ and so $m + n = x \in \mathfrak{L} \cap \mathfrak{M} + \mathfrak{L} \cap \mathfrak{N}$.

Something interesting about subspaces, resembling vectors, is that

$$\begin{aligned} \mathfrak{A}, \mathfrak{B} \subseteq V \implies \\ \mathfrak{A} + \mathfrak{B} \subseteq V. \end{aligned}$$

Just change $\subseteq$ for $\in$ and let $\mathfrak{A}, \mathfrak{B}$ be vectors to note the resemblance. $\square$