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

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

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. $\square$

(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, $-x = (-1) \cdot x$. $\square$

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

Proof. Note that

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

$\square$

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

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