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 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.