

Selected Solutions to Paul R. Halmos's
Finite-Dimensional Vector Spaces Second Edition

Greg Kikola

July 13, 2019

Contents

1	Spaces	1
1.1	Fields	1
1.4	Vector Spaces, Examples, and Comments	7

Chapter 1

Spaces

1.1 Fields

1.1.1 Exercise 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. By the commutativity of addition and the definition of 0,

$$0 + \alpha = \alpha + 0 = \alpha. \quad \square$$

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

Proof. Adding $-\alpha$ to both sides of the first equation gives

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

which by associativity and commutativity of addition gives

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

and by definition of additive inverses, this gives

$$0 + \beta = 0 + \gamma \quad \text{or} \quad \beta = \gamma,$$

making use of the fact that $0 + \delta = \delta$ for any $\delta \in \mathcal{F}$ (already proven above). \square

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

Proof. This follows from commutativity and associativity of addition:

$$\alpha + (\beta - \alpha) = \alpha + (-\alpha + \beta) = (\alpha - \alpha) + \beta = 0 + \beta = \beta. \quad \square$$

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

Proof. By definition of 0 and 1 and by distributivity we have

$$\alpha \cdot 0 = \alpha(1 - 1) = \alpha \cdot 1 - \alpha \cdot 1 = \alpha - \alpha = 0.$$

By commutativity of multiplication, $0 \cdot \alpha = 0$ as well. \square

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

Proof. From the various field axioms we have

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

\square

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

Proof. Since

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

it follows that $(-1)(-1)$ is an additive inverse of -1 . Since additive inverses are unique, we have $(-1)(-1) = 1$. Using this fact along with the previous result and with commutativity and associativity of multiplication we have

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

as desired. \square

(g) If $\alpha\beta = 0$, then either $\alpha = 0$ or $\beta = 0$ (or both).

Proof. Let $\alpha\beta = 0$. If $\alpha = 0$ then we are done, so suppose α is nonzero. Then α has a unique multiplicative inverse α^{-1} . Multiplying both sides of the original equation by this inverse gives

$$\alpha^{-1}(\alpha\beta) = \alpha^{-1} \cdot 0$$

which gives

$$(\alpha^{-1}\alpha)\beta = 0.$$

And since $\alpha^{-1}\alpha = \alpha\alpha^{-1} = 1$ we have $\beta = 0$ which completes the proof. \square

1.1.2 Exercise 2

- (a) Is the set of all positive integers a field?

Solution. The set of positive integers (note that Halmos defines this set as including 0) is not a field because, for example, 1 does not have an additive inverse in this set. \square

- (b) What about the set of all integers?

Solution. The set of all integers is not a field since, for example, 2 does not have a multiplicative inverse in the set. \square

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

Solution. Yes, though the operations can become rather complicated. For example, we can form a bijection (a one-to-one correspondence) f between the integers and the rationals since both are countable sets. Then define addition of integers \oplus and multiplication of integers \otimes by

$$\alpha \oplus \beta = f^{-1}(f(\alpha) + f(\beta))$$

and

$$\alpha \otimes \beta = f^{-1}(f(\alpha) \cdot f(\beta)),$$

where $+$ and \cdot indicate the usual operations on the rationals. Since the rationals form a field, it is not difficult to show that the binary operations \oplus and \otimes make the integers into a field with $f^{-1}(0)$ taking the role of the additive identity and $f^{-1}(1)$ taking the role of the multiplicative identity. \square

1.1.3 Exercise 3

Let m be an integer, $m \geq 2$, and let \mathcal{Z}_m be the set of all positive integers less than m ,

$$\mathcal{Z}_m = \{0, 1, \dots, m-1\}.$$

If α and β are in \mathcal{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 positive remainder obtained by dividing the (ordinary) product of α and β by m .

- (a) Prove that \mathcal{Z}_m is a field if and only if m is a prime.

Proof. Note that addition and multiplication, as defined here, are both closed since dividing by m will always produce a remainder between 0 and $m-1$. Note also that commutativity, associativity, and distributivity of these operations follow from the respective properties of ordinary addition and multiplication (for example, dividing $\alpha + \beta$ by m produces the same remainder as dividing $\beta + \alpha$ by m).

Also note that \mathbb{Z}_m contains the additive identity 0 and the multiplicative identity 1, since $\alpha + 0$, when divided by m , always produces the remainder α and similarly for 1α . We also have additive inverses since $-\alpha$ divided by m produces a remainder of $m - \alpha$, so that $\alpha + -\alpha = \alpha + (m - \alpha)$ gives the expected remainder 0.

Therefore, to show that \mathbb{Z}_m is a field, we only need show that every nonzero element has a multiplicative inverse.

We will make use of some results from number theory. Suppose m is prime. Then for any nonzero $\alpha \in \mathbb{Z}_m$, the greatest common divisor of α and m must be 1. By Bézout's Identity, there exist integers x and y such that

$$\alpha x + my = 1,$$

(we are here using ordinary addition and multiplication). Then $\alpha x = -my + 1$, and it follows that αx , when divided by m , leaves a remainder of 1. Therefore we can take α^{-1} to be the least positive remainder of dividing x by m .

Finally, to show the converse, note that if $m = ab$ where $a, b > 1$, then $a, b \in \mathbb{Z}_m$ but $ab = 0$. By an earlier result (Exercise 1.1.1), if \mathbb{Z}_m is a field, then $ab = 0$ implies that $a = 0$ or $b = 0$, which is a contradiction. Therefore \mathbb{Z}_m is not a field in this case. \square

- (b) What is -1 in \mathbb{Z}_5 ?

Solution. The additive inverse of 1 in \mathbb{Z}_5 is 4, since $1 + 4 = 0$. \square

- (c) What is $\frac{1}{3}$ in \mathbb{Z}_7 ?

Solution. The multiplicative inverse of 3 in \mathbb{Z}_7 is 5 since $3 \cdot 5 = 1$. Therefore $1 \cdot 3^{-1} = 1 \cdot 5 = 5$. \square

1.1.4 Exercise 4

The example of \mathbb{Z}_p (where p is prime) shows that not quite all the laws of elementary arithmetic hold in fields; in \mathbb{Z}_2 , for instance, $1 + 1 = 0$. Prove that if \mathcal{F} is a field, then either the result of repeatedly adding 1 to itself is always different from 0, or else the first time that it is equal to 0 occurs when the number of summands is a prime. (The *characteristic* of the field \mathcal{F} is defined to be 0 in the first case and the crucial prime in the second.)

Proof. For this exercise, let $n \cdot \alpha$ represent the result of adding α to itself n times, where n is an ordinary strictly positive integer and α is in the field \mathcal{F} . If $n \cdot 1$ is never 0 for any n then we are done, so suppose there is some particular n such that $n \cdot 1 = 0$. Obviously $n > 1$ since the additive and multiplicative identities in a field are distinct by definition.

Suppose $n = ab$, so that $(ab) \cdot 1 = 0$. But $a \cdot (b \cdot 1) = 0$ also, since adding 1 to itself b times, taking the result, and adding it to itself a times is the same as just adding 1 to itself ab times.

Let $c = b \cdot 1$. By distributivity, we can see that

$$a \cdot c = \overbrace{c + c + c + \cdots + c}^{a \text{ terms}} = c \overbrace{(1 + 1 + 1 + \cdots + 1)}^{a \text{ terms}} = c(a \cdot 1).$$

Therefore $(b \cdot 1)(a \cdot 1) = 0$, and since $b \cdot 1$ and $a \cdot 1$ are both in \mathcal{F} , we see that either $b \cdot 1 = 0$ or $a \cdot 1 = 0$.

Now, find the prime factorization of n so that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad \text{where } p_i \text{ is prime and } e_i \geq 1 \text{ for each } i.$$

From the above argument, we know that either $p_1 \cdot 1 = 0$, or $p_2 \cdot 1 = 0$, \dots , or $p_k \cdot 1 = 0$. And each p_i is smaller than n (unless n is itself prime), so this shows that no matter what value of n we choose such that $n \cdot 1 = 0$, we can always find a smaller prime p so that $p \cdot 1 = 0$. Therefore the smallest possible n must be prime, which completes the proof. \square

1.1.5 Exercise 5

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

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

Solution. Since

$$(\alpha_1 + \beta_1\sqrt{2}) + (\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)\sqrt{2}$$

this shows that $a + b \in \mathcal{Q}(\sqrt{2})$ whenever a and b are themselves members. Similarly

$$(\alpha_1 + \beta_1\sqrt{2})(\alpha_2 + \beta_2\sqrt{2}) = (\alpha_1\alpha_2 + 2\beta_1\beta_2) + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{2},$$

so multiplication is also closed.

Multiplicative inverses exist since if $\alpha + \beta\sqrt{2}$ is nonzero, then

$$(\alpha + \beta\sqrt{2}) \left(\frac{\alpha}{\alpha^2 - 2\beta^2} + \frac{-\beta}{\alpha^2 - 2\beta^2}\sqrt{2} \right) = \frac{(\alpha + \beta\sqrt{2})(\alpha - \beta\sqrt{2})}{\alpha^2 - 2\beta^2} = 1.$$

The remaining properties follow from the properties of the rationals, with $0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$ taking their usual roles. Therefore $\mathcal{Q}(\sqrt{2})$ is indeed a field. \square

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

Solution. If α and β must be integers, then the resulting set does not form a field since $2 = 2 + 0\sqrt{2}$ (for example) does not have a multiplicative inverse. \square

1.1.6 Exercise 6

- (a) Does the set of all polynomials with integer coefficients form a field?

Solution. If the set (call it $\mathbb{Z}[x]$) did form a field, 1 would have to be the multiplicative identity. But there is no polynomial which, when multiplied by the polynomial x , gives 1 (that is, $1/x$ is not a polynomial). Since there is a nonzero element in $\mathbb{Z}[x]$ which does not have a multiplicative inverse, $\mathbb{Z}[x]$ cannot be a field. \square

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

Solution. This set is still not a field for the same reason. \square

1.1.7 Exercise 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?

Solution. If \mathcal{F} were to be a field with the above operations, then the additive identity would have to be $(0, 0)$ and the multiplicative identity would be $(1, 1)$. But then, for example, the element $(0, 1)$ would have no multiplicative inverse since for all real a and b , $(a, b)(0, 1) = (0, b) \neq (1, 1)$. It follows that \mathcal{F} is not a field. \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?

Solution. Yes, \mathcal{F} is a field in this case. In fact, \mathcal{F} is isomorphic to the complex numbers \mathbb{C} (this is actually one way of defining the complex numbers). Here $(0, 0)$ takes the role of the additive identity, $(1, 0)$ takes the role of the multiplicative identity, and any complex number $a + bi$ corresponds to the element (a, b) in \mathcal{F} . \square

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

Solution. In the first case \mathcal{F} is not a field for the same reason given above. The second case is more interesting, but it is not a field either. Consider,

$$(1, i)(1, -i) = (1 - 1, 0) = (0, 0).$$

In this case we see that \mathcal{F} has two nonzero elements whose product is zero, but this is not possible for a field, as was proven in Exercise 1.1.1. \square

1.4 Vector Spaces, Examples, and Comments

1.4.1 Exercise 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. This follows directly from the commutativity of addition of vectors along with the definition of the vector 0 . \square

(b) $-0 = 0$.

Proof. By definition of 0 , we have $-0 + 0 = -0$. But the left-hand side is equal to 0 by definition of additive inverses, so $0 = -0$. \square

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

Proof. Since $0 = 0 + 0$, we have by distributivity that

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

Adding $-(\alpha \cdot 0)$ to both sides then gives $0 = \alpha \cdot 0$ as desired. \square

(d) $0 \cdot x = 0$.

Proof. The proof is similar to the previous one, except that the 0 on the left is a scalar:

$$0x = (0 + 0)x = 0x + 0x,$$

and adding $-(0x)$ to both sides gives the desired result. \square

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

Proof. Let $\alpha x = 0$. If $\alpha = 0$ then we are done, so suppose α is nonzero. Then $\alpha \in \mathcal{F}$ has an inverse α^{-1} . Multiplying both sides of $\alpha x = 0$ by α^{-1} then gives

$$\alpha^{-1}(\alpha x) = \alpha^{-1} \cdot 0,$$

which implies

$$1x = x = 0,$$

completing the proof. \square

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

Proof. By distributivity we have

$$x + (-1)x = 1x + (-1)x = (1 + -1)x = 0x = 0.$$

Now adding $-x$ to both sides and simplifying gives $(-1)x = -x$ as required. \square

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

Proof. Using commutativity and associativity of addition gives

$$y + (x - y) = (y + (-y)) + x = 0 + x = x. \quad \square$$

1.4.2 Exercise 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. Since \mathbb{Z}_p has p members, the number of possible vectors is p^n . \square

1.4.3 Exercise 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

$$x + y = (\xi_1 + \eta_1, \xi_2 + \eta_2)$$

$$\alpha x = (\alpha \xi_1, 0)$$

$$0 = (0, 0)$$

$$-x = (-\xi_1, -\xi_2).$$

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

Solution. \mathcal{V} is not a vector space since $1x \neq x$ when ξ_2 is nonzero. \square

1.4.4 Exercise 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. To check whether a subset \mathcal{V} of a vector space is a subspace, we only need to ensure three things: that the subset \mathcal{V} is nonempty, that for all $x, y \in \mathcal{V}$ also $x + y \in \mathcal{V}$, and that for all $\alpha \in \mathcal{F}$ and $x \in \mathcal{V}$ also $\alpha x \in \mathcal{V}$. It is then easy to check that all of the axioms hold. For example, since \mathcal{V} must be nonempty, we can take $x \in \mathcal{V}$ so that $0x = 0 \in \mathcal{V}$. The other properties are similar.

- (a) This is a vector space over \mathcal{R} since it is nonempty, it is closed under vector addition, and it is closed under scalar multiplication.

However, this is not a vector space over the field \mathbb{C} since scalar multiplication is not closed. For example, $(1, 1, 1) \in \mathcal{V}$ but $i(1, 1, 1) \notin \mathcal{V}$.

- (b) $0 \in \mathcal{V}$ so \mathcal{V} is nonempty. For any $x = (0, \xi_2, \xi_3)$ and $y = (0, \eta_2, \eta_3) \in \mathcal{V}$ we have $x + y \in \mathcal{V}$ so \mathcal{V} is closed under addition. And for any $\alpha \in \mathbb{C}$ we have $\alpha x = (0, \alpha \xi_2, \alpha \xi_3) \in \mathcal{V}$ so \mathcal{V} is closed under scalar multiplication. Therefore \mathcal{V} is a vector space.

- (c) Since $(1, 0, 0) \in \mathcal{V}$ and $(0, 1, 0) \in \mathcal{V}$ but their sum $(1, 1, 0) \notin \mathcal{V}$, we see that \mathcal{V} is not a vector space.
- (d) This \mathcal{V} is obviously not closed under scalar multiplication, so it cannot be a vector space.
- (e) This \mathcal{V} does not contain the zero vector, so it cannot be a vector space. \square

1.4.5 Exercise 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 3,
- (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. (a) This \mathcal{V} is not closed under addition. For example, the polynomials t^3 and $-t^3 + t^2$ are both in \mathcal{V} but their sum is not (it has degree 2).

- (b) \mathcal{V} is nonempty since $0 \in \mathcal{V}$. Suppose $x, y \in \mathcal{V}$. Then

$$2(x + y)(0) = 2(x(0) + y(0)) = 2x(0) + 2y(0) = x(1) + y(1) = (x + y)(1)$$

and for any $\alpha \in \mathbb{C}$,

$$2(\alpha x)(0) = 2\alpha(x(0)) = \alpha(2x(0)) = \alpha(x(1)) = (\alpha x)(1).$$

Therefore \mathcal{V} is a vector space.

- (c) This \mathcal{V} is not closed under scalar multiplication. For example, $t \in \mathcal{V}$ but $(-1)t = -t \notin \mathcal{V}$.
- (d) $0 \in \mathcal{V}$ so \mathcal{V} is nonempty. And for any $x, y \in \mathcal{V}$ and $\alpha \in \mathbb{C}$, we have

$$(x + y)(t) = x(t) + y(t) = x(1 - t) + y(1 - t) = (x + y)(1 - t)$$

and

$$(\alpha x)(t) = \alpha(x(t)) = \alpha(x(1 - t)) = (\alpha x)(1 - t),$$

so \mathcal{V} is a vector space. \square