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

Greg Kikola

July 12, 2019

Contents

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,

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

(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:

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

(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. □

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

Proof. From the various field axioms we have

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

□

(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. □

(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. □

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. □

(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. □

(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. □

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 $\mathcal{Z}_m$ 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 $\mathcal{Z}_m$ 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 $\alpha \in \mathcal{Z}_m$, 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 $a, b \in \mathcal{Z}_m$ but $ab = 0$. By an earlier result (Exercise 1.1.1), if Z_m is a field, then $ab = 0$ implies that $a = 0$ or $b = 0$, which is a contradiction. Therefore Z_m is not a field in this case. □

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

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

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

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

1.1.4 Exercise 4

The example of $\mathcal{Z}_p$ (where p is prime) shows that not quite all the laws of elementary arithmetic hold in fields; in $\mathcal{Z}_2$, 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 $p_2 \cdot 1 = 0$, ..., 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. □

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. □

(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. □

1.1.6 Exercise 6

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

Solution. If the set (call it $\mathcal{Z}[x]$) 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 $\mathcal{Z}[x]$ which does not have a multiplicative inverse, $\mathcal{Z}[x]$ cannot be a field. □

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

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

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. □

(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 $\mathcal{C}$ (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 $\mathcal{F}$. □

(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. □