Notes on "Finite-Dimensional Vector Spaces" by Paul R. Halmos

October 1, 2022

Each `\section` corresponds to the scope of one member's assignment, and each `\subsection` corresponds to one theorem or exercise in the textbook, specified in the format $m.n$ where m is the section number and n is the theorem/exercise number. If n is not given, we use $n = 1$ instead.

1 Toga (2022/09/19)

1.1 Exercise 1.1

(a) Since addition is commutative, $0+\alpha = \alpha+0$ holds. We also have $\alpha+0 = \alpha$ by definition, hence $0 + \alpha = \alpha$.

2 Mohehe (2022/09/27)

2.1 Exercise 1.1

(b) If $\alpha + \beta = \alpha + \gamma$, we have $\beta = \beta + 0 = 0 + \beta = (\alpha + (-\alpha)) + \beta = ((-\alpha) + \alpha) + \beta = (-\alpha) + (\alpha + \beta) = (-\alpha) + (\alpha + \gamma) = ((-\alpha) + \alpha) + \gamma = (\alpha + (-\alpha)) + \gamma = 0 + \gamma = \gamma + 0 = \gamma$ by definition. Therefore, $\beta = \gamma$ holds.

(c) We have $\alpha+(\beta-\alpha) = \alpha+(\beta+(-\alpha)) = \alpha+((-\alpha)+\beta) = (\alpha+(-\alpha))+\beta = 0 + \beta = \beta + 0 = \beta$ by definition. Therefore, $\alpha + (\beta - \alpha) = \beta$ holds.

(d) We have $\alpha 0 + \alpha 0 = \alpha(0 + 0) = \alpha 0 = \alpha + 0$ by definition, hence $\alpha 0 = 0$ by Exercise 1(b). We also have $\alpha \cdot 0 = 0 \cdot \alpha$ by definition. Therefore, $\alpha \cdot 0 = 0 \cdot \alpha = 0$

(e) We have $\alpha+(-1)\alpha = 1\alpha+(-1)\alpha = (1+(-1))\alpha = 0\alpha = 0$ by definition and Exercise 1(d). Since the additive inverse is unique, we obtain $(-1)\alpha = -\alpha$.

(f) We have $(-\alpha)(-\beta) = ((-1)\alpha)((-1)\beta) = (\alpha(-1))((-1)\beta) = \alpha((-1)((-1)\beta)) = \alpha((-1)(-1)\beta)$ by Exercise 1(e) and definition. We also have $(-1)(-1) = 0 + (-1)(-1) = (1 + (-1)) + (-1)(-1) = 1 + (-1) + (-1)(-1) = 1 +$

$(-1)((-1)+1) = 1 + (-1)(1 + (-1)) = 1 + (-1)0 = 1 + 0 = 1$ by definition. By it and definition, $\alpha((-1)(-1)\beta) = \alpha(1\beta) = \alpha(\beta 1) = \alpha\beta$ holds. Therefore, $(-\alpha)(-\beta) = \alpha\beta$ holds.

(g) If $\alpha\beta = 0$, suppose $\alpha \neq 0$ and $\beta \neq 0$ hold. By supposition and definition, we have $0 = \alpha^{-1}0 = \alpha^{-1}(\alpha\beta) = (\alpha^{-1}\alpha)\beta = (\alpha\alpha^{-1})\beta = 1\beta = \beta 1 = \beta$, hence $\beta = 0$. However, this result contradicts supposition, "$\alpha \neq 0$ and $\beta \neq 0$". Therefore, if $\alpha\beta = 0$, then either $\alpha = 0$ or $\beta = 0$ (or both).

3 Joh (2022/09/19)

3.1 Exercise 1.2

(a) The set of positive integers is not a field since there is no additive inverse for 1.

(b) The set of integers is not a field since there is no multiplicative inverse for 2.

(c) There exists a bijective map φ from $\mathbb{N}$ (or $\mathbb{Z}$) to $\mathbb{Q}$ [1], where $\mathbb{Q}$ is a field [2]. We can make $\mathbb{N}$ a field by re-defining (i) addition by $a \oplus b = \varphi^{-1}(\varphi(a) + \varphi(b))$ and (ii) multiplication by $a \otimes b = \varphi^{-1}(\varphi(a)\varphi(b))$ for each $a, b \in \mathbb{N}$. Note that the additive and multiplicative identities become $\varphi^{-1}(0)$ and $\varphi^{-1}(1)$, respectively. For each $\alpha \in \mathbb{N}$, the additive inverse becomes $\varphi^{-1}(-\varphi(\alpha))$, and the multiplicative inverse becomes $\varphi^{-1}(1/\varphi(\alpha))$ if $\alpha \neq \varphi^{-1}(0)$.

Let $\alpha, \beta, \gamma, \alpha', \beta' \in \mathbb{N}$. Note that
1) $\alpha \oplus \beta = \varphi^{-1}(\varphi(\alpha) + \varphi(\beta)) = \varphi^{-1}(\varphi(\beta) + \varphi(\alpha)) = \beta \oplus \alpha$ holds.(addition is commutative)
(from here, mohehe)
2) $\alpha \oplus (\beta \oplus \gamma) = \alpha \oplus (\varphi^{-1}(\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha) + \varphi(\varphi^{-1}(\varphi(\beta) + \varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha) + (\varphi(\beta) + \varphi(\gamma))) = \varphi^{-1}((\varphi(\alpha) + \varphi(\beta)) + \varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha) + \varphi(\beta))) + \varphi(\gamma)) = \varphi^{-1}(\varphi(\alpha) + \varphi(\beta)) \oplus \gamma = (\alpha \oplus \beta) \oplus \gamma$ holds.(addition is associative)
3) $\alpha \oplus \varphi^{-1}(0) = \varphi^{-1}(\varphi(\alpha) + \varphi(\varphi^{-1}(0))) = \varphi^{-1}(\varphi(\alpha) + 0) = \varphi^{-1}(\varphi(\alpha)) = \alpha$ holds.(there exists additive identity, $\varphi^{-1}(0)$) If α' and β' are additive identity, we have $\alpha' = \alpha' \oplus \beta' = \beta' \oplus \alpha' = \beta'$ by 1) and the definition of additive identity.(additive identity is unique)
4) $-\varphi(\alpha) \in \mathbb{Q}$ holds by definition, so $\varphi^{-1}(-\varphi(\alpha)) \in \mathbb{N}$ holds. Therefore, $\alpha \oplus \varphi^{-1}(-\varphi(\alpha)) = \varphi^{-1}(\varphi(\alpha) + \varphi(\varphi^{-1}(-\varphi(\alpha)))) = \varphi^{-1}(\varphi(\alpha) + (-\varphi(\alpha))) = \varphi^{-1}(0)$ holds.(for each α ($\alpha \in \mathbb{N}$), there exists additive inverse) For each α, if α' and β' are additive inverse, we have $\alpha' = \alpha' \oplus \varphi^{-1}(0) = \alpha' \oplus (\alpha \oplus \beta') = (\alpha' \oplus \alpha) \oplus \beta' = (\alpha \oplus \alpha') \oplus \beta' = \varphi^{-1}(0) \oplus \beta' = \beta \oplus \varphi^{-1}(0) = \beta'$ by 1), 2), 3) and the definition of additive inverse.(additive inverse is unique)
5) $\alpha \otimes \beta = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)) = \varphi^{-1}(\varphi(\beta)\varphi(\alpha)) = \beta \otimes \alpha$ holds.(multiplication is commutative)

6) $\alpha \otimes (\beta \otimes \gamma) = \alpha \otimes (\varphi^{-1}(\varphi(\beta)\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(\varphi(\beta)\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)\varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\beta)))\varphi(\gamma)) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)) \otimes \gamma = (\alpha \otimes \beta) \otimes \gamma$ holds.(multiplication is associative)
7) $\alpha \otimes \varphi^{-1}(1) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(1))) = \varphi^{-1}(\varphi(\alpha) \cdot 1) = \alpha$ holds.(there exists additive identity, $\varphi^{-1}(1)$) If α' and β' are additive identity, we have $\alpha' = \alpha' \otimes \beta' = \beta' \otimes \alpha' = \beta'$ by 5) and definition of multiplicative identity.(multiplicative identity is unique)
8) For each α ($\alpha \neq \varphi^{-1}(0)$), $(1/\varphi(\alpha)) \in \mathbb{Q}$ holds by definition, so $\varphi^{-1}(1/\varphi(\alpha)) \in \mathbb{N}$ holds. Therefore, $\alpha \otimes \varphi^{-1}(1/\varphi(\alpha)) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(1/\varphi(\alpha)))) = \varphi^{-1}(\varphi(\alpha)(1/\varphi(\alpha))) = \varphi^{-1}(1)$ holds.(for each α ($\alpha \in \mathbb{N}$), there exists multiplicative inverse) For each α ($\alpha \neq \varphi^{-1}(0)$), if α' and β' are multiplicative inverse, we have $\alpha' = \alpha' \otimes \varphi^{-1}(1) = \alpha' \otimes (\alpha \otimes \beta') = (\alpha' \otimes \alpha) \otimes \beta' = (\alpha \otimes \alpha') \otimes \beta' = \varphi^{-1}(1) \otimes \beta' = \beta' \otimes \varphi^{-1}(1) = \beta'$ by 5), 6), 7) and the definition of multiplicative inverse.(multiplicative inverse is unique)
9) $\alpha \otimes (\beta \oplus \gamma) = \alpha \otimes (\varphi^{-1}(\varphi(\beta)+\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\varphi^{-1}(\varphi(\beta)+\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha)(\varphi(\beta)+\varphi(\gamma))) = \varphi^{-1}(\varphi(\alpha)\varphi(\beta)+\varphi(\alpha)\varphi(\gamma)) = \varphi^{-1}(\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\beta)))+\varphi(\varphi^{-1}(\varphi(\alpha)\varphi(\gamma)))) = \varphi^{-1}(\varphi(\alpha \otimes \beta)+\varphi(\alpha \otimes \gamma)) = \alpha \otimes \beta \oplus \alpha \otimes \gamma$ holds.(distributive law stands)

4 Mohehe

4.1 Exercise 1.3

For two integers a and b, we denote by $a \,\%\, b$ the remainder after dividing a by b, and write $b \mid a$ if and only if $a \,\%\, b = 0$. For clarity, we denote the ordinary sum and product of two integers a and b by $a +_{\mathbb{Z}} b$ and $a \cdot_{\mathbb{Z}} b$, respectively. Note that $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \,\%\, m$ and $\alpha\beta = (\alpha \cdot_{\mathbb{Z}} \beta) \,\%\, m$ for $\alpha, \beta \in \mathcal{Z}_m$.

(a) Let $\alpha, \beta, \gamma \in \mathcal{Z}_m$, $k \in \mathbb{Z}$
 Proof : if m is a prime, $\mathcal{Z}_m$ is a field.
 Suppose m is a prime,

1) $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \,\%\, m = (\beta +_{\mathbb{Z}} \alpha) \,\%\, m = \beta + \alpha$ (addition is commutative)
2) Since $\alpha +_{\mathbb{Z}} (\beta + \gamma) = \alpha +_{\mathbb{Z}} (\beta +_{\mathbb{Z}} \gamma) \,\%\, m \equiv \alpha +_{\mathbb{Z}} (\beta +_{\mathbb{Z}} \gamma) = (\alpha +_{\mathbb{Z}} \beta) +_{\mathbb{Z}} \gamma \equiv (\alpha +_{\mathbb{Z}} \beta) \,\%\, m +_{\mathbb{Z}} \gamma = (\alpha + \beta) +_{\mathbb{Z}} \gamma \pmod m$ holds, $\alpha + (\beta + \gamma) = (\alpha +_{\mathbb{Z}} (\beta + \gamma)) \,\%\, m = ((\alpha + \beta) +_{\mathbb{Z}} \gamma) \,\%\, m = (\alpha + \beta) + \gamma$ holds.(addition is associative)
3) $\alpha + 0 = (\alpha +_{\mathbb{Z}} 0) \,\%\, m = \alpha \,\%\, m = \alpha$ (there exists additive identity) By it and 1), if β and γ are additive identity, $\beta = \beta + \gamma = \gamma + \beta = \gamma$ (additive identity is unique)
4) if $\alpha +_{\mathbb{Z}} \beta = m$, $\alpha + \beta = (\alpha +_{\mathbb{Z}} \beta) \,\%\, m = m \,\%\, m = 0$ (there exists additive inverse)
5) $\alpha\beta = (\alpha \cdot_{\mathbb{Z}} \beta) \,\%\, m = (\beta \cdot_{\mathbb{Z}} \alpha) \,\%\, m = \beta\alpha$ (multiplication is commutative)
6) Since $\alpha \cdot_{\mathbb{Z}} (\beta\gamma) = \alpha \cdot_{\mathbb{Z}} ((\beta \cdot_{\mathbb{Z}} \gamma) \,\%\, m) \equiv \alpha \cdot_{\mathbb{Z}} (\beta \cdot_{\mathbb{Z}} \gamma) = (\alpha \cdot_{\mathbb{Z}} \beta) \cdot_{\mathbb{Z}} \gamma \equiv ((\alpha \cdot_{\mathbb{Z}} \beta) \,\%\, m) \cdot_{\mathbb{Z}} \gamma = (\alpha\beta) \cdot_{\mathbb{Z}} \gamma \pmod m$ holds, $\alpha(\beta\gamma) = (\alpha \cdot_{\mathbb{Z}} (\beta\gamma)) \,\%\, m = ((\alpha\beta) \cdot_{\mathbb{Z}} \gamma) \,\%\, m = (\alpha\beta)\gamma$ holds.(multiplication is associative)

7) $\alpha 1 = (\alpha_{\mathbb{Z}} 1) \,\%\, m = \alpha \,\%\, m = \alpha$ (there exists multiplicative identity) By it and 5), if β and γ are multiplicative identity, $\beta = \beta\gamma = \gamma\beta = \gamma$ (multiplicative identity is unique)

8) For all $\alpha(\alpha \neq 0)$, suppose there doesn't exist β that makes $\alpha\beta = 1$. There exists $\alpha\beta = \alpha\gamma$ $(\beta \neq \gamma)$, because β is any one from 0 to $m-1$ and $\alpha\beta$ is any one from 0 to $m-1$ except 1. Therefore, $(\alpha \cdot_{\mathbb{Z}} \beta +_{\mathbb{Z}} (-\alpha \cdot_{\mathbb{Z}} \gamma) =)\ \alpha \cdot_{\mathbb{Z}} (\beta +_{\mathbb{Z}} (-\gamma)) = km$ holds. The right side has divisor m, but it contradicts that the left side doesn't have divisor of m except 1, because $0 < \alpha < (m-1)$ and $((-m) < (\beta +_{\mathbb{Z}} (-\gamma)) < 0$ or $0 < (\beta +_{\mathbb{Z}} (-\gamma)) < m)$ holds. Thus, there exists β that makes $\alpha\beta = 1$.(there exists maltiplicative inverse)

9) $\alpha(\beta+\gamma) = (\alpha \cdot_{\mathbb{Z}} (\beta+\gamma)) \,\%\, m = (\alpha \cdot_{\mathbb{Z}} ((\beta +_{\mathbb{Z}} \gamma) \,\%\, m)) \,\%\, m \equiv (\alpha \cdot_{\mathbb{Z}} (\beta +_{\mathbb{Z}} \gamma)) \,\%\, m = (\alpha \cdot_{\mathbb{Z}} \beta + \alpha \cdot_{\mathbb{Z}} \gamma) \,\%\, m \equiv ((\alpha \cdot_{\mathbb{Z}} \beta) \,\%\, m +_{\mathbb{Z}} (\alpha \cdot_{\mathbb{Z}} \gamma) \,\%\, m) \,\%\, m \equiv (\alpha \cdot \_Z\beta) \,\%\, m + (\alpha \cdot_{\mathbb{Z}} \gamma) \,\%\, m \equiv \alpha\beta + \alpha\gamma$ holds.(distributive law stands)

In conclusion, if m is a prime, $\mathcal{Z}_m$ is a field.

Proof : If $\mathcal{Z}_m$ is a field, m is a prime.
By contraposition, it is equivalent to prove "If m is not a prime, $\mathcal{Z}_m$ is not a field." We can prove 1) to 7) and 9) by the same way. For all $\alpha(\alpha \neq 0)$, suppose there exists β that makes $\alpha\beta = 1$. If $m = 4$ and $\alpha = 2$, $\alpha 0 = 0, \alpha 1 = 2, \alpha 2 = 0, \alpha 3 = 2$, but it contradicts that there exists β that makes $\alpha\beta = 1$. Therefore there exists α that doesn't have β that makes $\alpha\beta = 1$. In conclusion, "If m is not a prime, $\mathcal{Z}_m$ is not a field." and "If $\mathcal{Z}_m$ is a field, m is a prime."

Therefore $\mathcal{Z}_m$ is a field if and only if m is a prime.

(b) 4

(c) 5

4.2 Exercise 1.4

Define $\alpha_0, \alpha_1, \ldots, \in \mathfrak{F}$ as below:

$$\alpha_0 = 0, \tag{1}$$
$$\alpha_n = \alpha_{n-1} + 1 \qquad (n > 0). \tag{2}$$

We have $\alpha_m \alpha_n = \alpha_{mn}$ for all m and n. Assume there exists an n with $\alpha_n = 0$ but $\alpha_k \neq 0$ for any $k < n$. It suffices to prove that n is a prime.

References

[1] https://proofwiki.org/wiki/Rational_Numbers_are_Countably_Infinite

[2] https://proofwiki.org/wiki/Rational_Numbers_form_Field